ОКБ ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

Модуль доверенной загрузки «Аккорд-МКТ»

Руководство администратора

37222406.501410.071 90
37222406.26.20.40.140.082 90
37222406.26.20.40.140.112 90

Листов 77

Москва
2026

АННОТАЦИЯ

Настоящий документ является руководством администратора на изделие «Модуль доверенной загрузки «Аккорд-МКТ» (далее по тексту – изделие «Аккорд-МКТ», Изделие, «Аккорд-МКТ», МДЗ «Аккорд-МКТ») и предназначен для конкретизации задач и функций должностных лиц организации (предприятия, фирмы), планирующих и организующих защиту информации в системах и средствах информатизации на базе СВТ с применением МДЗ «Аккорд-МКТ».

В документе приведены основные функции, особенности настройки и эксплуатации МДЗ «Аккорд-МКТ», основные функции администратора МДЗ «Аккорд-МКТ» и сведения, необходимые для управления защитными механизмами МДЗ «Аккорд-МКТ».

Перед настройкой и эксплуатацией МДЗ «Аккорд-МКТ» необходимо внимательно ознакомиться с комплектом эксплуатационной документации, а также принять необходимые защитные организационные меры, рекомендуемые в документации.

Применение защитных средств МДЗ «Аккорд-МКТ» должно дополняться общими мерами технической безопасности.

СОДЕРЖАНИЕ

ПРИНЯТЫЕ ТЕРМИНЫ И ОБОЗНАЧЕНИЯ

Администратор БИ (или АБИ) – администратор безопасности информации, привилегированный пользователь – должностное лицо, имеющее особый статус и абсолютные полномочия (супервизора). Администратор БИ планирует защиту информации на предприятии (учреждении, фирме и т.д.), определяет права доступа пользователям в соответствии с утвержденным Планом защиты, организует настройку МДЗ «Аккорд-МКТ», эксплуатацию и контроль правильности его использования, осуществляет периодическое тестирование средств защиты МДЗ «Аккорд-МКТ».

Доверенная загрузка – загрузка ОС только после проведения контрольных процедур идентификации/аутентификации пользователей, проверки целостности объектов по спискам контроля.

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.

Ошибки – информация, выводимая на дисплей, указывающая на неправильность действий, сбои, аварии МДЗ «Аккорд-МКТ».

Сертификат ЭП – сертификат проверки электронной подписи, содержит набор атрибутов открытого ключа, используемого для двухфакторной аутентификации пользователя. Хранится в базе данных МДЗ «Аккорд-МКТ».

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

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ	- автоматизированное рабочее место
АС	- автоматизированная система
ЗБ	- задание по безопасности
МДЗ	- модуль доверенной загрузки
НСД	- несанкционированный доступ к информации
ОС	- операционная система
ПО	- программное обеспечение
ПС	- программные средства
РД	- руководящий документ
СДЗ	- средство доверенной загрузки
СЗИ	- средства защиты информации
СПО	- системное программное обеспечение
ТУ	- технические условия
ФПО	- функциональное программное обеспечение
ЭД	- эксплуатационная документация
ЭП	- электронная подпись

1. Общие сведения

1.1. Назначение

Модуль доверенной загрузки «Аккорд-МКТ» является программным средством доверенной загрузки (СДЗ), предназначенным для встраивания в базовую систему ввода-вывода (БСВВ, далее - BIOS) ЭВМ на базе процессоров с архитектурой x86_64 (ТУ 501410-071-37222406-2016, ТУ 26.20.40.140-082-37222406-2019, ТУ 26.20.40.140-112-37222406-2023) и микрокомпьютеров на базе процессоров с архитектурой ARM (ТУ 501410-071-37222406-2016) и обеспечения выполнения основных функций ее защиты от НСД, в том числе настройки, контроля функционирования и управления защитными механизмами.

МДЗ «Аккорд-МКТ» обеспечивает:

- идентификацию и аутентификацию пользователей при входе в систему по уникальному идентификатору пользователя и по паролю временного действия длиной от 0 до 63 буквенно-цифровых символов, введенных с клавиатуры;
- идентификацию и аутентификацию пользователей при допуске к средствам настройки и администрирования МДЗ «Аккорд-МКТ» по уникальному идентификатору пользователя и по паролю 0 до 63 буквенно-цифровых символов, введенных с клавиатуры;
- контроль целостности отдельных файлов, ветвей реестра и программных средств ЭВМ;
- администрирование, включающее:
    - регистрацию пользователей и их идентификаторов;
    - 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.

1.2. Состав МДЗ «Аккорд-МКТ»

МДЗ «Аккорд-МКТ» является программным продуктом, предназначенным для встраивания в BIOS ЭВМ на базе процессоров с архитектурой x86_64 (ТУ 501410-071-37222406-2016, ТУ 26.20.40.140-082-37222406-2019, ТУ 26.20.40.140-112-37222406-2023) и микрокомпьютеров на базе процессоров с архитектурой ARM (ТУ 501410-071-37222406-2016) и состоит из специального программного обеспечения «Аккорд-МКТ» (далее по тексту СПО «Аккорд-МКТ»).

Встраивание (прошивка) СПО «Аккорд-МКТ» в BIOS выполняется производителем изделия на этапе производства ЭВМ.

1.3. Условия применения МДЗ «Аккорд-МКТ»

СПО «Аккорд-МКТ» встраивается производителем в BIOS ЭВМ на этапе изготовления и функционирует в ее составе. Возможен также вариант самостоятельной установки МДЗ «Аккорд-МКТ» пользователем (ТУ 26.20.40. 140-112-37222406-2023).

СВТ с установленным на нем МДЗ «Аккорд-МКТ» может использоваться в качестве подконтрольного объекта для удаленного управления с помощью СПО «Аккорд-РАУ» или СКРД Diamond ACS.

Применяемое на СВТ с МДЗ «Аккорд-МКТ» USB-устройство «USB-ДСЧ.РКБ» (ТУ 26.12.1-069-37222406-2024) в формате аппаратного сторожевого таймера позволяет повысить его защищенность.

Для корректной работы МДЗ «Аккорд-МКТ» необходимо обеспечить функционирование на ЭВМ только BIOS UEFI (ТУ 26.20.40.140-082-37222406-2019, ТУ 26.20.40.140-112-37222406-2023). Это достигается, например:

- использованием ЭВМ без модуля поддержки совместимости CSM;
- установкой в ЭВМ BIOS без модуля поддержки совместимости CSM;
- отключением в SetupBIOS модуля поддержки совместимости CSM и установкой пароля на вход в BIOS;
- устранением векторов угроз, связанных с модулем поддержки совместимости CSM, посредством его исключения из образа BIOS;
- иными способами на усмотрение эксплуатирующей организации.

Помимо этого, корректная работа МДЗ предполагает ограничение доступа пользователей к разделу диска с ПО МДЗ путем отключения диска в ОС.

Среда функционирования МДЗ «Аккорд-МКТ» запрещает любые действия от имени пользователя до завершения процедур его идентификации и аутентификации.

Среда функционирования МДЗ «Аккорд-МКТ» предоставляет надежные метки времени.

2. Функции безопасности, реализованные в МДЗ «Аккорд-МКТ»

МДЗ «Аккорд-МКТ» реализует следующие функции безопасности:

- разграничение доступа к управлению СДЗ;
- управление работой СДЗ;
- управление параметрами СДЗ;
- аудит безопасности СДЗ;
- идентификация и аутентификация;
- тестирование СДЗ, контроль целостности программного обеспечения и параметров СДЗ;
- контроль компонентов СВТ;
- блокирование загрузки операционной системы средством доверенной загрузки;
- сигнализация средства доверенной загрузки;
- обеспечение безопасности после завершения работы СДЗ.

Эти функции реализуются с помощью следующих механизмов:

- администрирование МДЗ - настройки, определяющие режим работы и произведенные пользователем из группы «Администраторы»;
- идентификация пользователя по его логину и аутентификация по паролю, введенному с клавиатуры;
- контроль целостности данных по спискам объектов контроля. Реализуется до загрузки ОС с помощью хэш-функции. В случае совпадения значений с эталонными процесс загрузки ОС продолжается, в противном случае загрузка приостанавливается;
- регистрация и учет в журнале регистрации следующих системных событий и действий пользователя:
  - начало сеанса пользователя;
  - прохождение процедуры идентификации/аутентификации пользователем;
  - создание журнала системных событий и действий пользователей;
  - изменение полномочий пользователей;
  - нарушения, выявленные в рамках контроля целостности данных по спискам объектов контроля.

3. Настройка МДЗ «Аккорд-МКТ»

Настройка МДЗ «Аккорд-МКТ» осуществляется обладающим соответствующими полномочиями администратором МДЗ «Аккорд-МКТ» и включает в себя:

1) установку параметров учетной записи «Гл. Администратор» (подробнее см. подраздел 5.2 настоящего Руководства);

2) регистрацию пользователей и настройку защитных средств МДЗ «Аккорд-МКТ» (подробнее см. соответствующие подразделы раздела 5 настоящего Руководства).

Перед проведением настройки необходимо убедиться в наличии всех необходимых отметок и подписей в разделе 5 («Свидетельство о приемке и маркировке») Формуляра на МДЗ «Аккорд-МКТ».

4. Функции и интерфейсы администрирования МДЗ «Аккорд-МКТ»

4.1. Функции администрирования

К функциям администрирования МДЗ «Аккорд-МКТ» относятся (подробнее см. соответствующие подразделы раздела 5):

- установка параметров учетной записи «Гл.Администратор» (задание идентификатора, установка пароля и т.п.);
- работа с учетными записями пользователей/ администраторов (создание/ удаление, настройка параметров);
- работа с группами пользователей/ администраторов (создание/ удаление, настройка параметров групп);
- настройки контроля целостности (файлов, реестра, загрузочных метаданных);
- просмотр/очистка системного журнала «Аккорд-МКТ»;
- общие настройки МДЗ «Аккорд-МКТ» (данные конфигурации);
- экспорт/импорт баз данных;
- форматирование баз данных МДЗ «Аккорд-МКТ»;
- регламентные проверки (проверка целостности ПО, проверка целостности данных).

4.2. Интерфейсы администрирования

Администрирование МДЗ «Аккорд-МКТ» выполняется с помощью графического интерфейса пользователя.

5. Управление МДЗ «Аккорд-МКТ» безопасным способом

ВНИМАНИЕ! Всем пользователям МДЗ «Аккорд-МКТ» (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 идентификаторы.

ВНИМАНИЕ! При каждом входе в среду администрирования МДЗ «Аккорд-МКТ» администратор обязан в первую очередь просмотреть системный журнал и проанализировать все события, произошедшие с момента его предыдущей авторизации. Только после этого администратор может приступить к другим своим обязанностям.

5.1. Начало работы

При первом запуске МДЗ «Аккорд-МКТ» выполняется его инициализация. После завершения этой операции на экран выводится главное окно среды администрирования (рисунки 1-5).

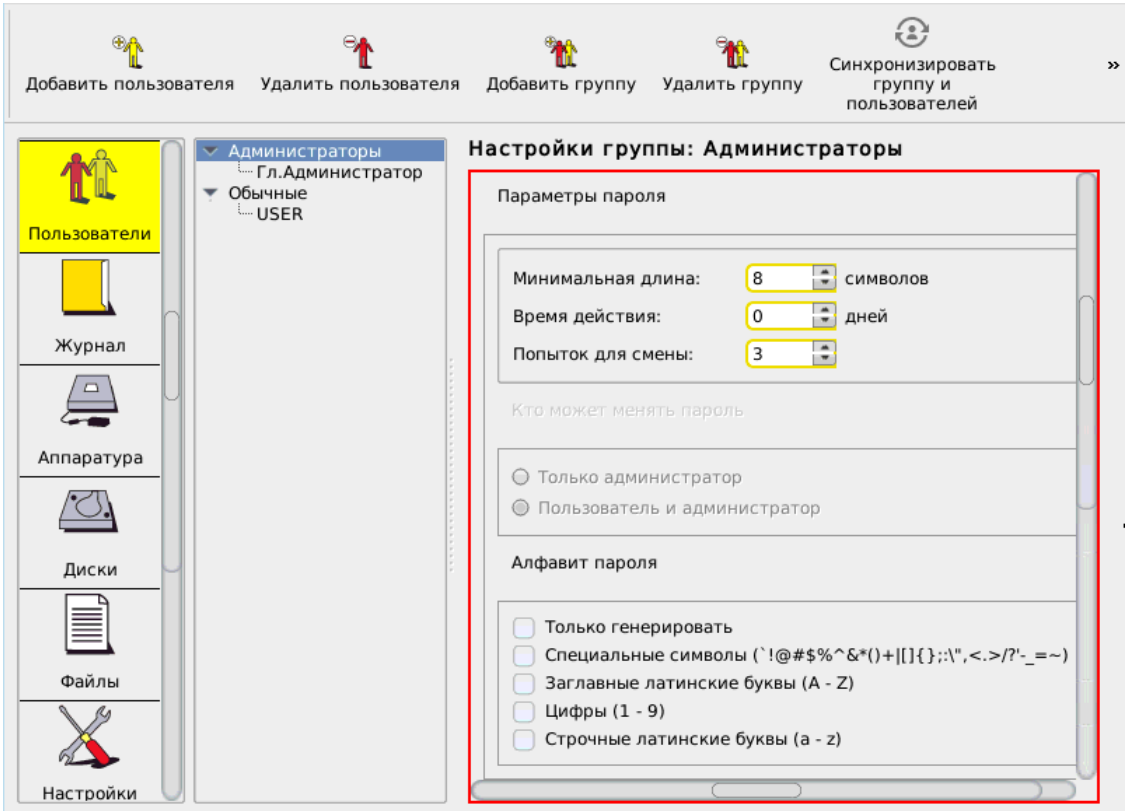

Рисунок 1 - Главное окно среды администрирования (ТУ 26.20.40.140-082-37222406-2019)

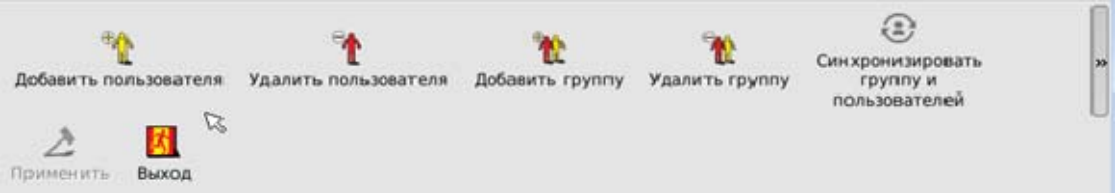

Рисунок 2 - Панель инструментов главного окна администрирования (ТУ 26.20.40.140-082-37222406-2019)

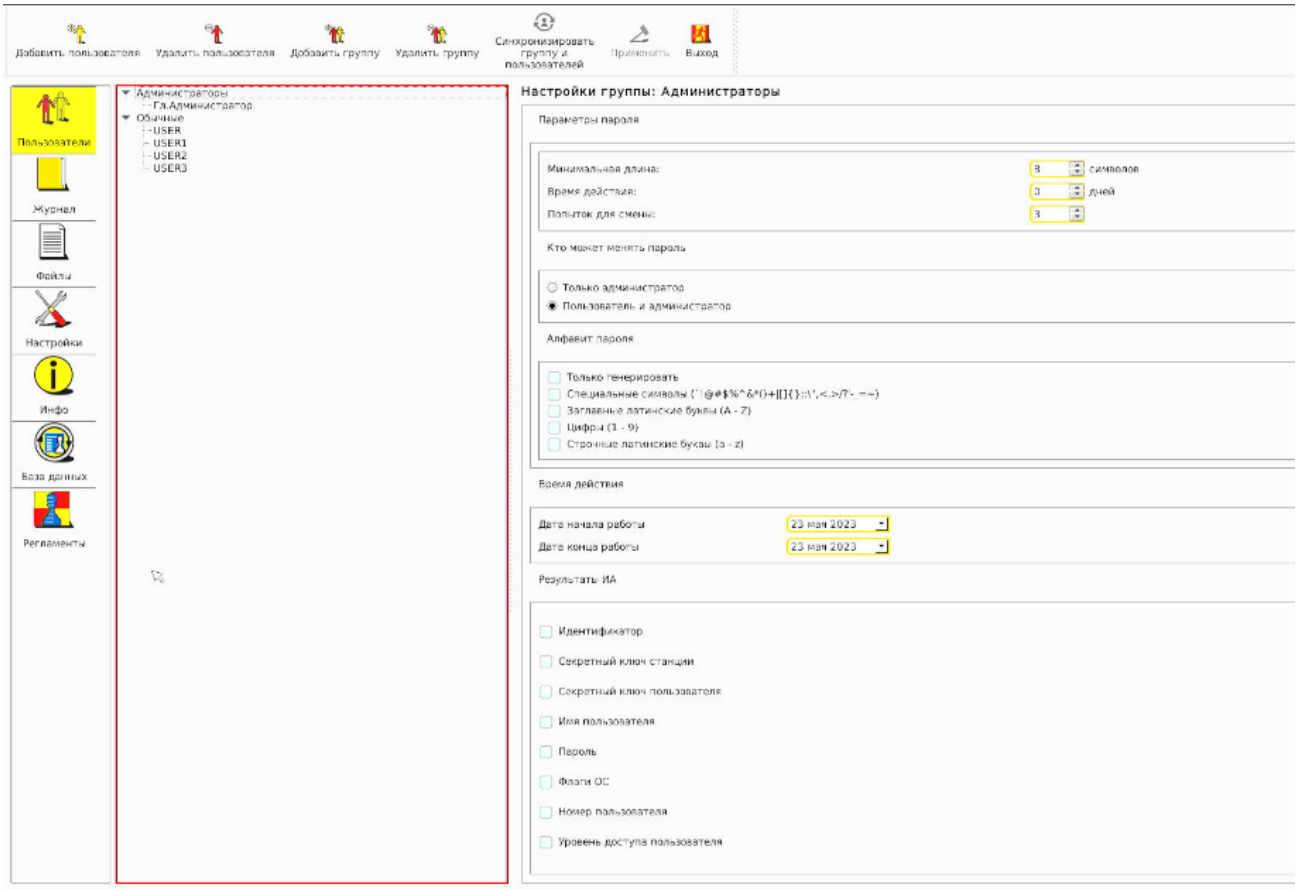

Рисунок 3 - Главное окно среды администрирования (ТУ 501410-071-37222406-2016)

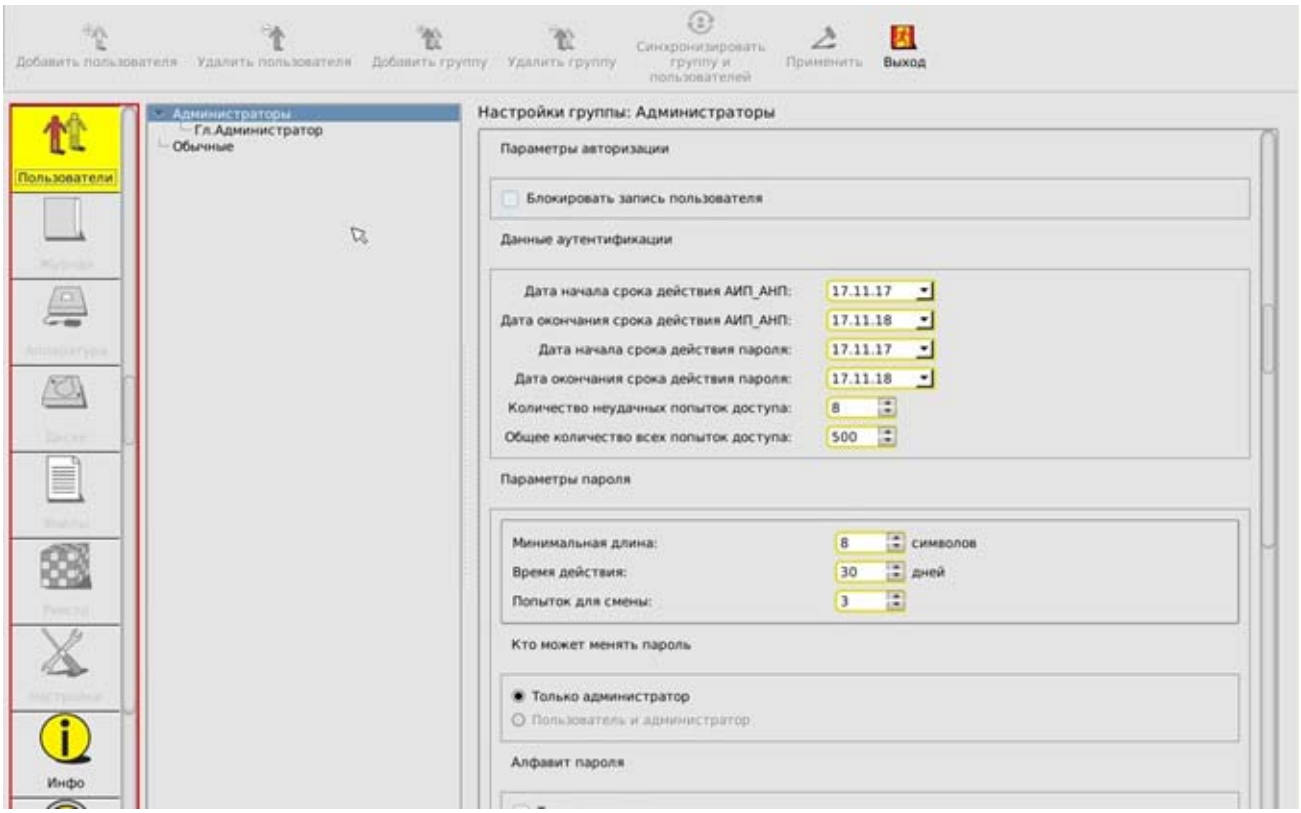

Рисунок 4 - Главное окно среды администрирования (ТУ 26.20.40.140-112-37222406-2023)

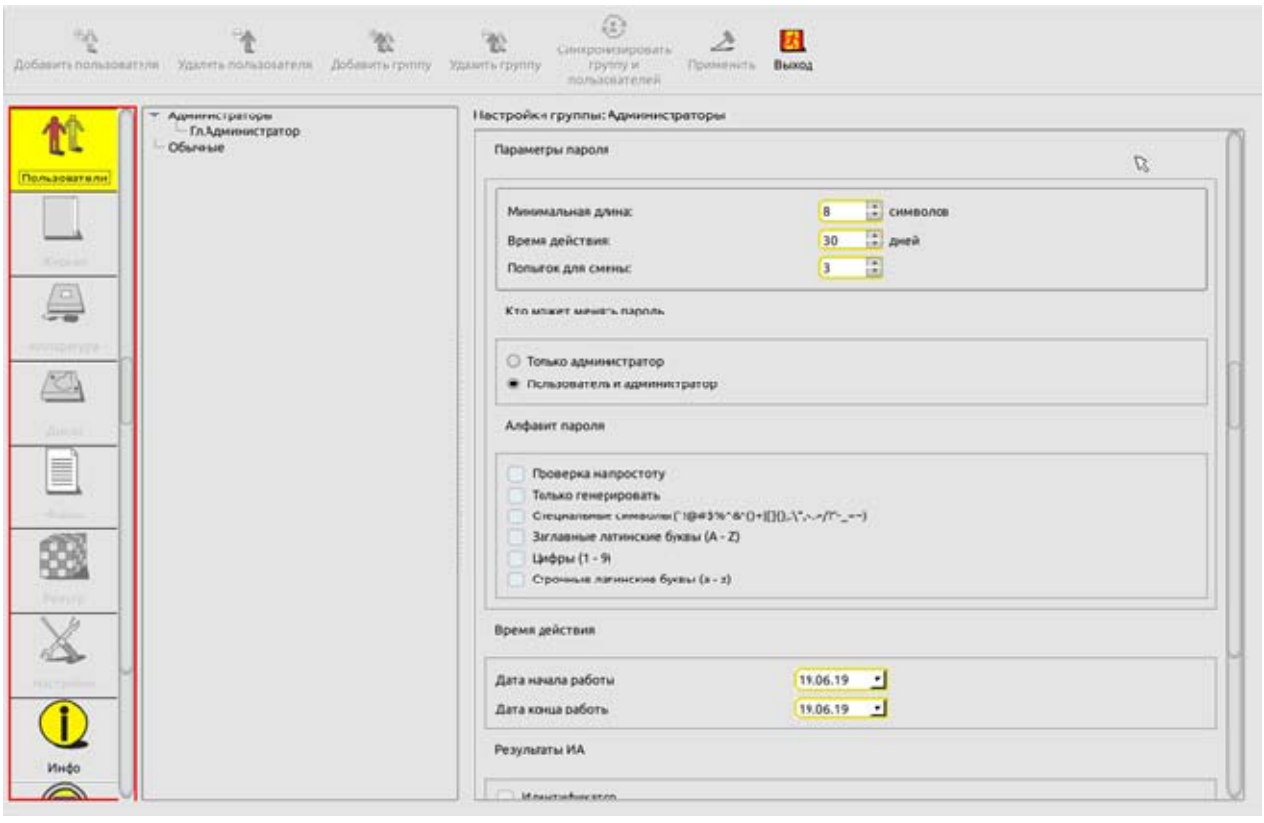

Рисунок 5 - Главное окно среды администрирования (ТУ 26.20.40.140-112-37222406-2023)

Главное окно среды администрирования состоит из следующих областей:

- меню выбора объектов администрирования (левая вертикальная панель);
- панель управления выбранным объектом администрирования:
  - панель инструментов (рисунок 2);
  - 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 по спискам объектов контроля;
- <Реестр> - контроль целостности разделов реестра Windows (ТУ 26.20.40.140-112-37222406-2023);
- <Настройки> - общие настройки МДЗ «Аккорд-МКТ»;
- <Инфо> - информация о версии прошивки МДЗ «Аккорд-МКТ» и контрольные суммы ядра защиты;
- <База данных> – выполнение процедур экспорта/импорта элементов базы данных;
- <Регламенты> – запуск процессов самотестирования МДЗ «Аккорд-МКТ».

В начале первого сеанса работы помимо главного окна среды администрирования на экран также выводится сообщение с требованием выполнить процедуру настройки параметров учетной записи Главного Администратора (рисунок 6), без выполнения которой недоступны никакие функции «Аккорд-МКТ».

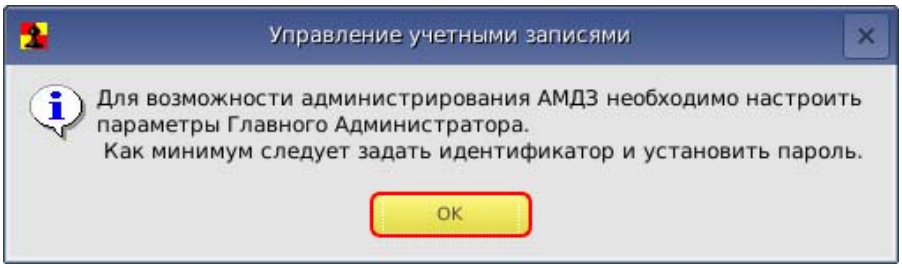

Рисунок 6 - Сообщение с требованием настроить параметры Главного Администратора

После выполнения процедуры установки параметров учетной записи Главного Администратора, описанной в подразделе 5.2 настоящего Руководства, функционал «Аккорд-МКТ» становится доступным для Главного Администратора.

Далее Главному Администратору следует зарегистрировать необходимое количество пользователей (или групп пользователей), настроить параметры их

учетных записей, а также списки контроля целостности (подробнее см. соответствующие подразделы настоящего Руководства).

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

5.2.1. Общие сведения

При инициализации МДЗ «Аккорд-МКТ» в базе данных создается учетная запись Главного Администратора (супервизора)[1] – «Гл. Администратор» – которому будут полностью доступны все функции администрирования. При этом для данного пользователя не установлены параметры учетной записи.

ВНИМАНИЕ! При первом старте «Аккорд-МКТ» прежде всего необходимо установить параметры учетной записи для пользователя «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».

В появившемся рабочем поле редактирования параметров учетной записи Главного Администратора (рисунок 7, рисунок 8) предварительно можно выполнить настройки следующих параметров:

- параметры пароля (см. подраздел 5.3.2.2);
- атрибуты доступа (см. подраздел 5.3.4.7).

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

[1)] В «Аккорд-МКТ» 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).

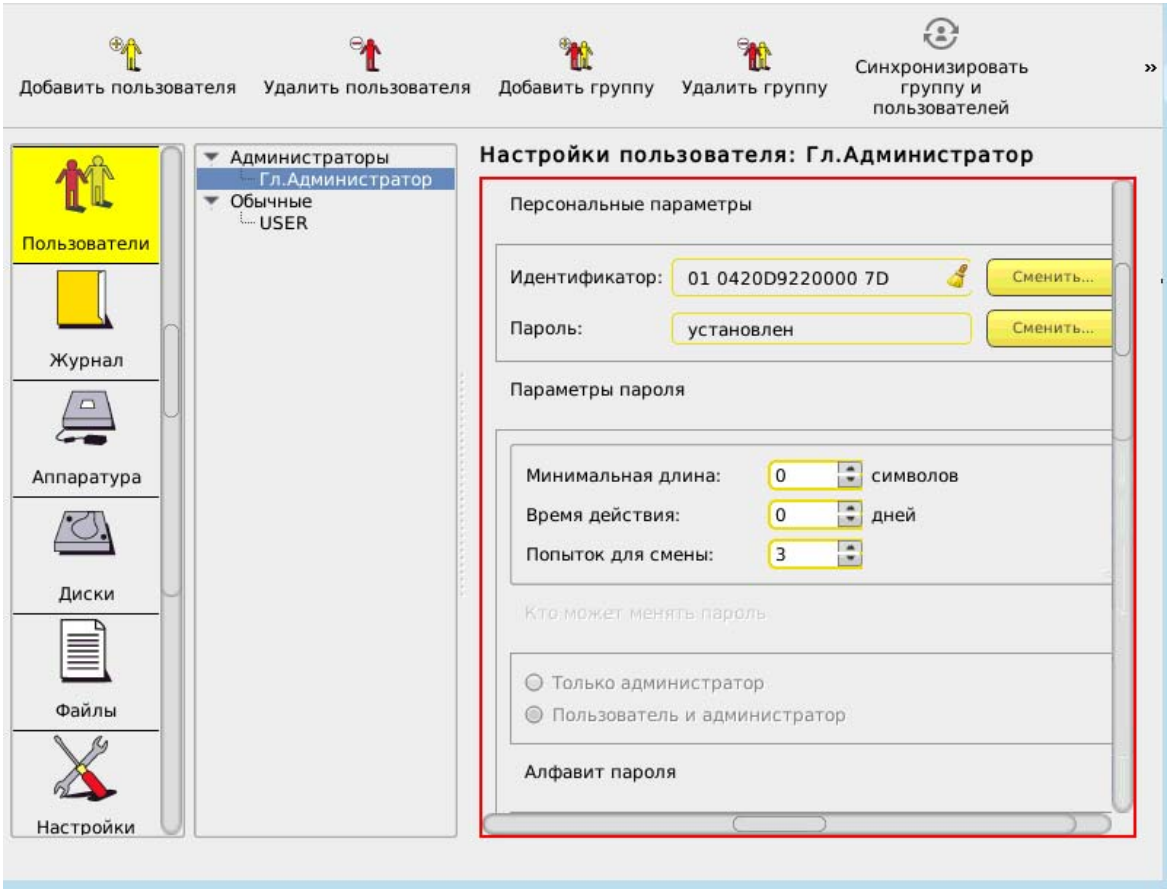

Рисунок 7 - Настройки пользователя «Гл. Администратор»

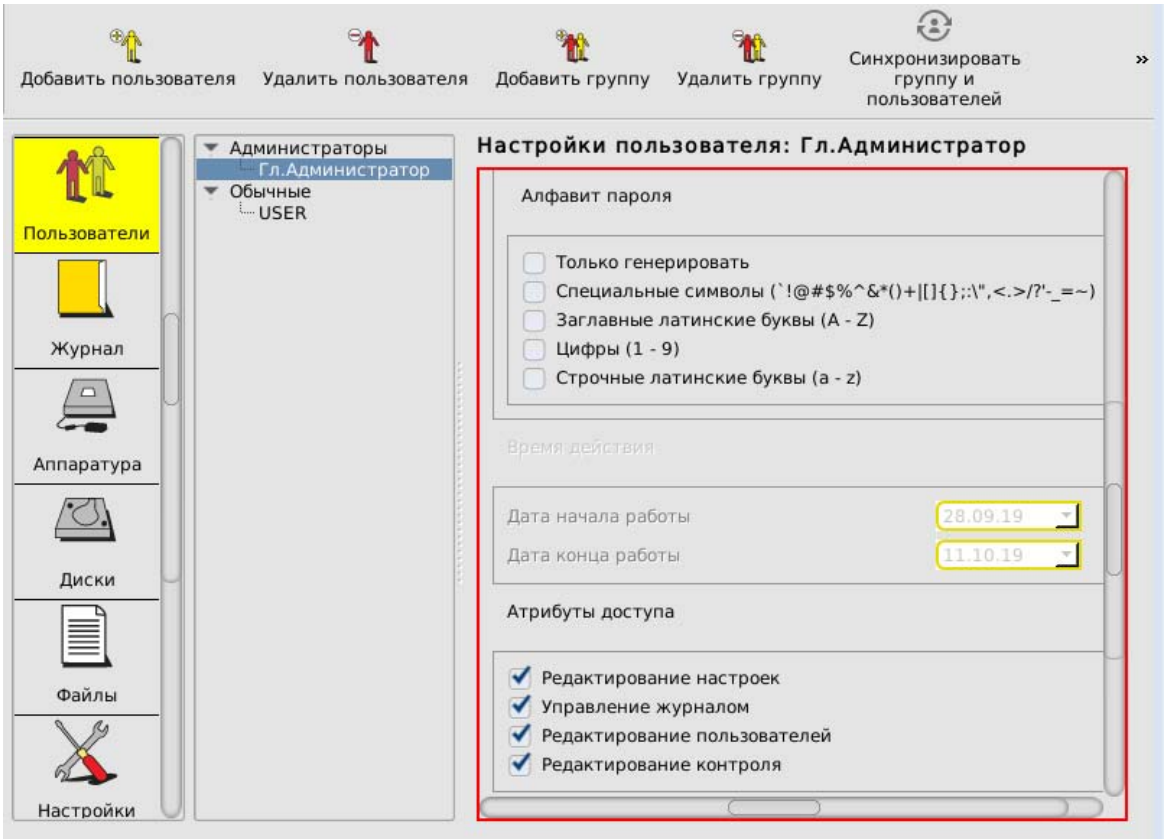

Рисунок 8 - Настройки пользователя «Гл. Администратор»

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

- данные аутентификации (ТУ 26.20.40.140-112-37222406-2023, см. п.4.2.2);
- идентификатор (см. п. 5.2.3);
- пароль (см. п. 5.2.4);
- время действия учетной записи (см. п. 5.3.2.3).

5.2.2. Настройка данных аутентификации (ТУ 26.20.40.140-112-37222406-2023)

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» (рисунок 4) следует настроить следующие параметры:

- «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.

5.2.3. Назначение идентификатора

Для регистрации идентификатора на правой панели в строке «Идентификатор» нужно нажать кнопку <Сменить> (рисунок 7).

В появившемся окне «Смена идентификатора» (рисунок 9) требуется указать, какой секретный ключ будет использоваться:

- Использовать существующий – подходит для аппаратных идентификаторов, которые используются в настоящий момент в

других СПО, а также для клавиатурного идентификатора[2], независимо от его использования в других СПО;

- Генерировать – подходит для клавиатурного идентификатора и аппаратных идентификаторов, которые не используются в настоящий момент в других СПО.

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.

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.

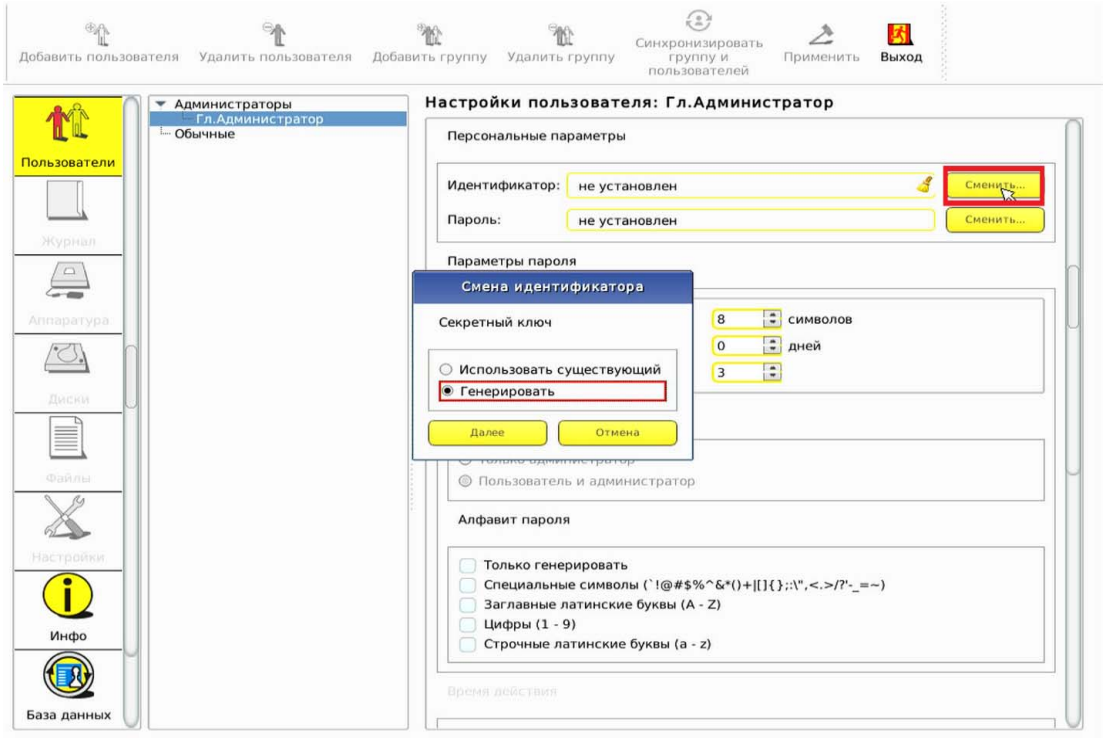

Рисунок 9 - Выбор режима для задания идентификатора

При выборе опции «Генерировать» и нажатии кнопки <Далее> в следующем окне следует ввести идентификатор в соответствующее поле с клавиатуры (рисунок 10), нажать <Enter> и далее <ОК>, или подключить аппаратный идентификатор в разъем на корпусе ЭВМ, дождаться заполнения поля «Идентификатор» (рисунок 11) и нажать кнопку <ОК>.

[2] Клавиатурный идентификатор используется только в СПО «Аккорд-МКТ» ТУ 26.20.40.140-071-37222406-2016 и ТУ 26.20.40.140-082-37222406-2019

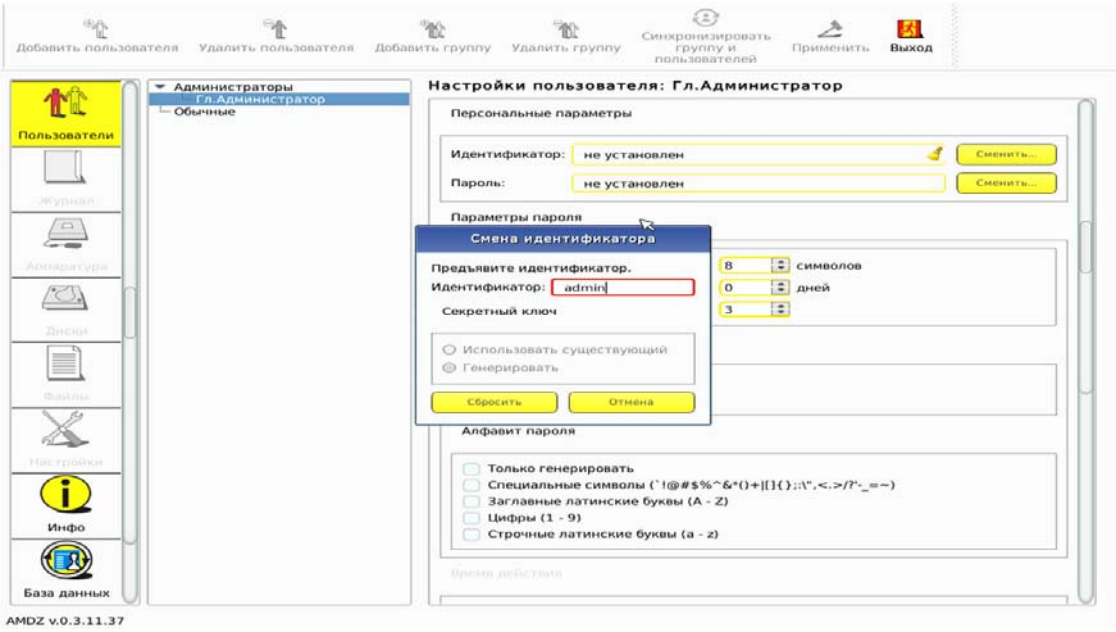

Рисунок 10 - Ввод идентификатора с клавиатуры

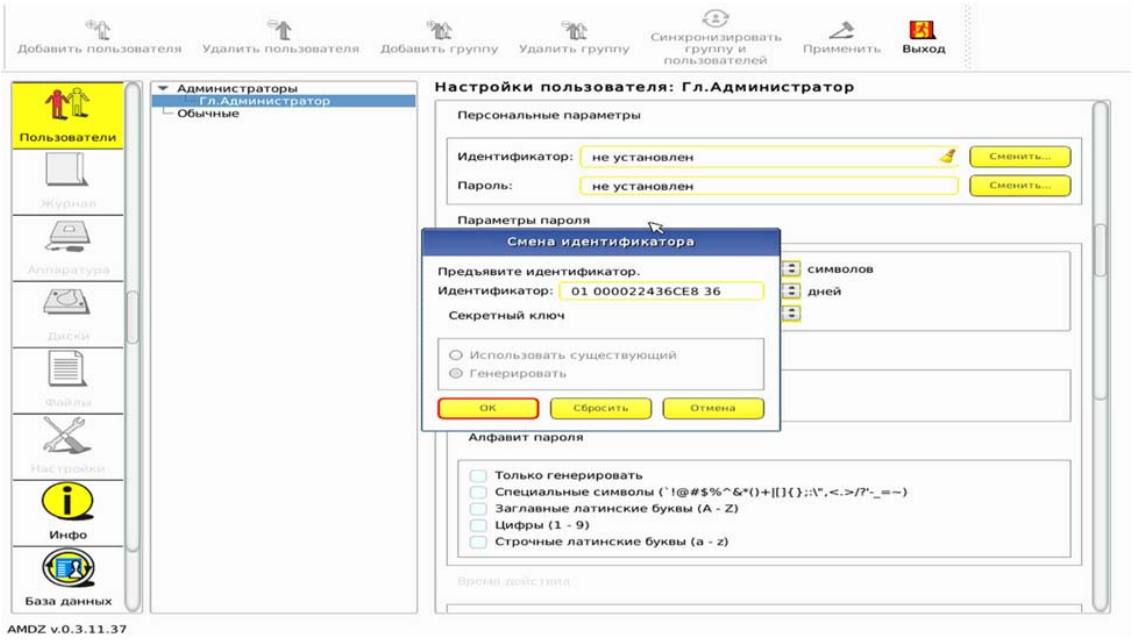

Рисунок 11 - Предъявление аппаратного идентификатора

При двухфакторной аутентификации по сертификатам ЭП в качестве идентификатора допускается использование USB-токенов как носителей закрытого ключа ЭП.

ВНИМАНИЕ! Попытка повторно назначить пользователю ранее назначенный идентификатор приведет к зависанию ЭВМ, которое устраняется только через переподключение питания.

По завершении процедуры задания идентификатора его значение появляется в поле «Идентификатор» главного окна среды администрирования.

Далее необходимо перейти к процедуре назначения пароля (см. 5.2.4) (для модели МДЗ «Аккорд-МКТ» ТУ 26.20.40.140-112-37222406-2023 процедура назначения пароля начинается автоматически по завершении процедуры назначения персонального идентификатора).

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 12), и программа ожидает от администратора завершения процедуры настройки параметров авторизации пользователя.

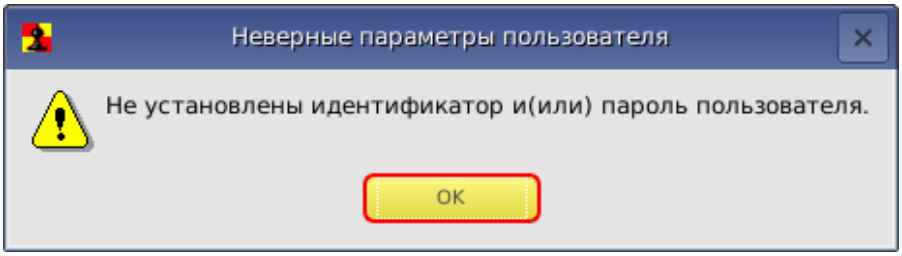

Рисунок 12 - Сообщение о том, что идентификатор или пароль пользователя не установлены

5.2.4. Назначение пароля

Перед выполнением процедуры назначения пароля на правой панели главного окна среды администрирования (рисунок 7) нужно установить необходимые параметры пароля (подробнее см. 5.3.2.2).

Выполнение процедуры назначения пароля начинается посредством нажатия кнопки <Сменить> в строке «Пароль» главного окна среды администрирования (рисунок 7) или автоматически по завершении процедуры назначения идентификатора (для модели МДЗ «Аккорд-МКТ» ТУ 26.20.40.140-112-37222406-2023).

На экран выводится окно ввода пароля (рисунок 13). При первоначальной регистрации параметров пользователя строка «Старый пароль» недоступна. Необходимо ввести новый пароль и подтвердить ввод пароля.

Пароль может состоять из букв, цифр и специальных символов (в зависимости от установленных администратором параметров пароля – см. 5.3.2.2). Вводимые символы на экране отображаются точками. При несовпадении введенных последовательностей выводится сообщение об ошибке. В этом случае операцию придется повторить. Символы могут вводиться как в верхнем, так и в нижнем регистре. Следует учитывать, что длина пароля должна быть не меньше параметра, установленного в строке «Минимальная длина» в разделе «Параметры пароля». Если длина введенного пароля меньше, выводится сообщение об ошибке. Не допускается ввод в качестве пароля

типичных последовательностей типа: '123456' или 'qwerty'. При вводе подобных последовательностей символов выдается сообщение об ошибке.

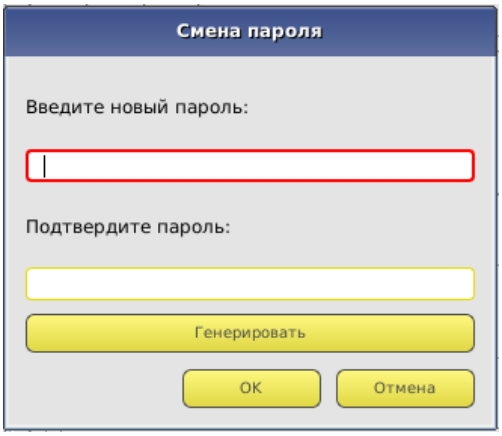

Рисунок 13 – Окно ввода пароля

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 12).

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» (рисунок 8). 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 7).

Для сохранения параметров пользователя «Гл.Администратор» нужно нажать кнопку <Применить> на панели инструментов вверху главного окна (рисунок 2).

После корректного выполнения описанной последовательности действий на экран выводится сообщение о сохранении внесенных изменений (рисунок 14).

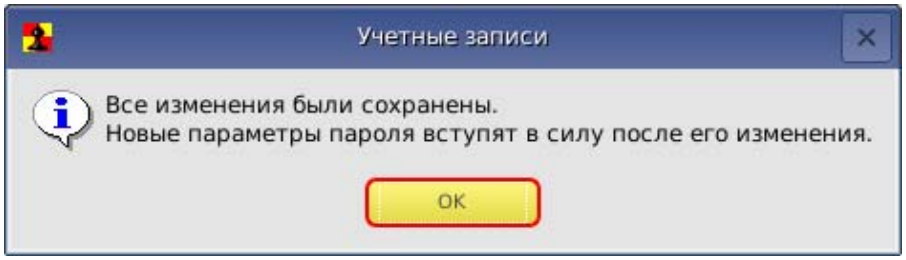

Рисунок 14 - Сообщение о сохранении внесенных изменений

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

5.3. Настройка параметров групп и учетных записей пользователей

5.3.1. Список пользователей

При инициализации МДЗ «Аккорд-МКТ» создаются две зарезервированные группы пользователей – «Администраторы» («ADMINS») и «Обычные» («EVERYONE»). 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.

5.3.2. Общие параметры группы «Администраторы»

5.3.2.1. Общие сведения

Для группы «Администраторы» установлены следующие общие параметры (рисунок 15, рисунок 16):

- параметры авторизации (см. 4.3.4.3, аналогично параметрам группы «Обычные»);
- данные аутентификации (ТУ 26.20.40.140-112-37222406-2023, см. 4.2.2);
- параметры пароля (см. 5.3.2.2);
- время действия (см. 5.3.2.3).

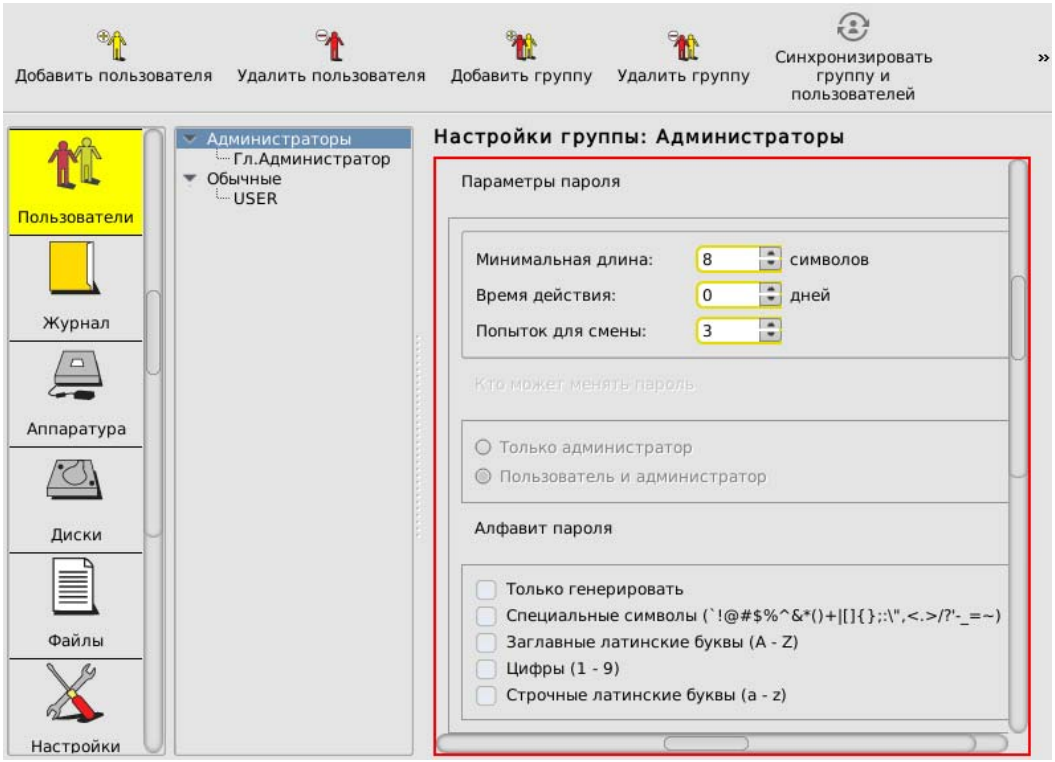

Рисунок 15 - Общие параметры группы «Администраторы»

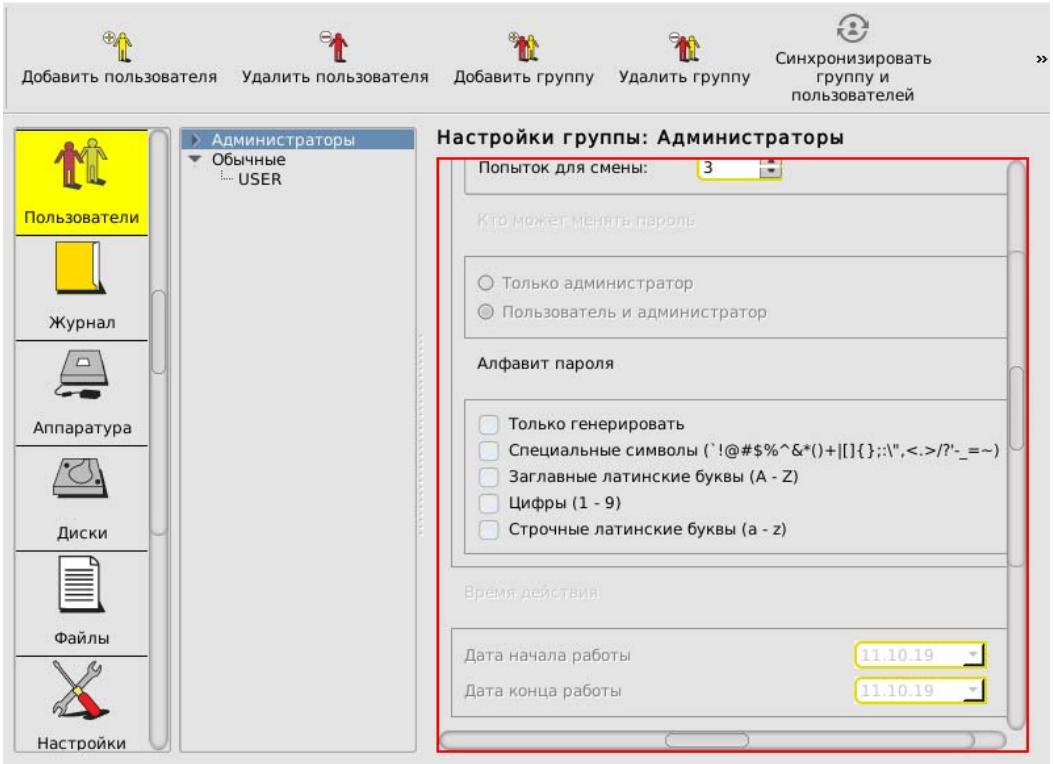

Рисунок 16 - Общие параметры группы «Администраторы»

5.3.2.2. Параметры пароля

Для управления парольной политикой можно регулировать следующие параметры пароля (рисунок 15):

- «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 - 63 символа.
- «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.
- «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.

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

5.3.2.3. Время действия

В разделе «Время действия» (рисунок 16) можно настроить следующие параметры:

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

Параметры раздела «Время действия» учитываются в процессе работы МДЗ «Аккорд-МКТ» только в том случае, если на вкладке «Настройки» в разделе «Данные конфигурации» (см. п. 5.13.1) администратором установлена галочка «Проверка времени действия учетной записи пользователя».

5.3.3. Общие параметры группы «Обычные» (пользователи)

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

– параметры авторизации (режим блокировки, см. 4.3.4.3);

– данные аутентификации (рисунок 18, ТУ 26.20.40.140-112-37222406-2023, см. 4.2.2,);

– параметры пароля (см. 5.3.2.2);

– время действия (см. 5.3.2.3).

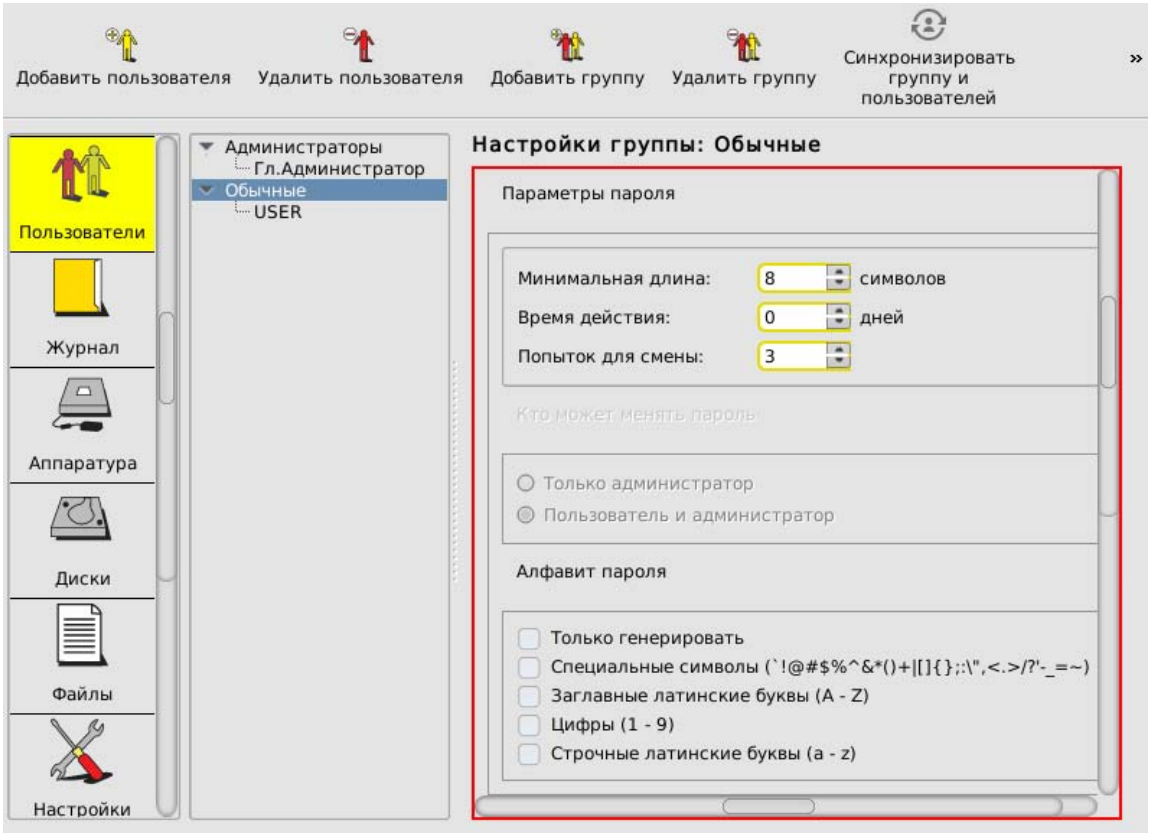

Рисунок 17 – Общие параметры группы «Обычные» (для моделей МДЗ «Аккорд-МКТ» ТУ 501410-071-37222406-2016, ТУ 501410-082-37222406-2019)

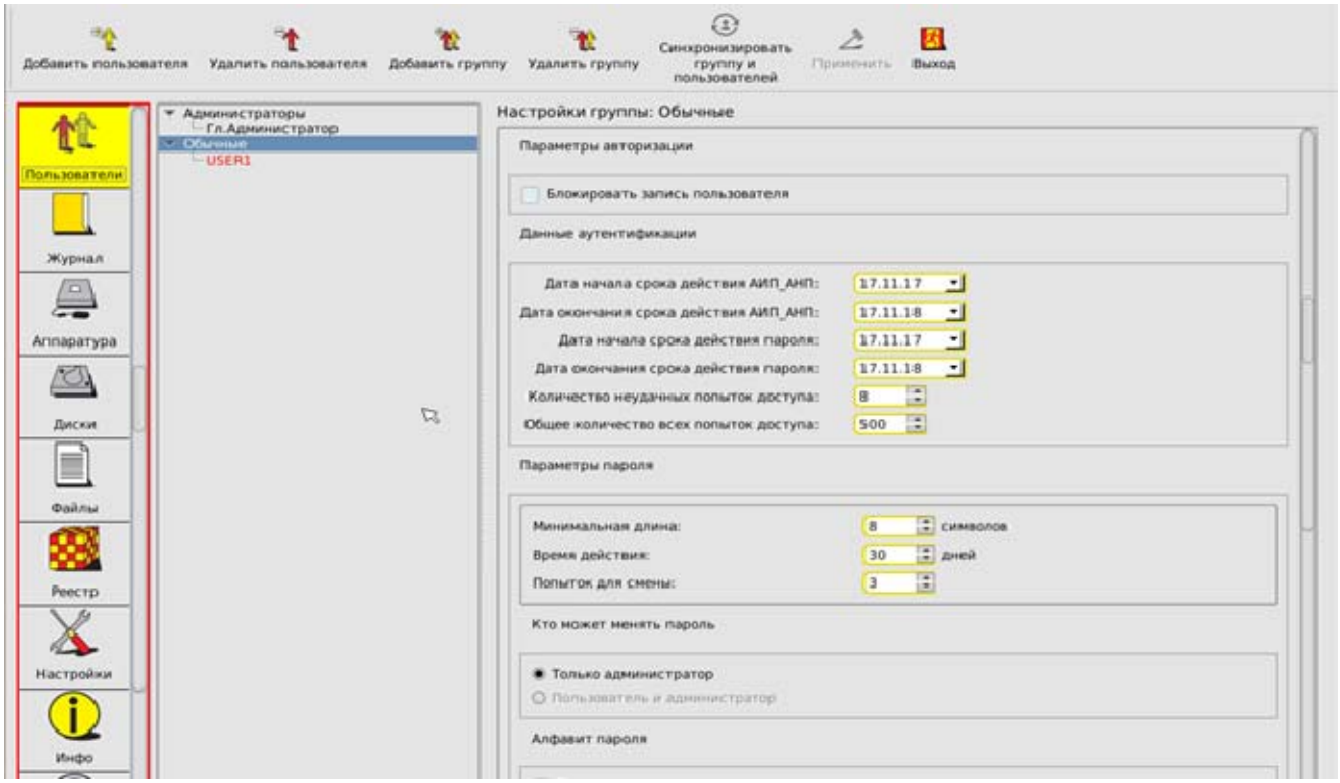

Рисунок 18 - Общие параметры группы «Обычные» (для модели МДЗ «Аккорд-МКТ» ТУ 501410-112-37222406-2023)

Настройки параметров аналогичны настройкам соответствующих общих параметров для группы «Администраторы».

5.3.4. Параметры пользователей в группе «Администраторы»

5.3.4.1. Общие сведения

Для пользователей группы «Администраторы» установлены следующие параметры (рисунок 19, рисунок 20):

- персональные параметры;
- параметры авторизации (режим блокировки);
- данные аутентификации (рисунок 21, ТУ 501410-112-37222406-2023);
- параметры пароля;
- время действия;
- атрибуты доступа.

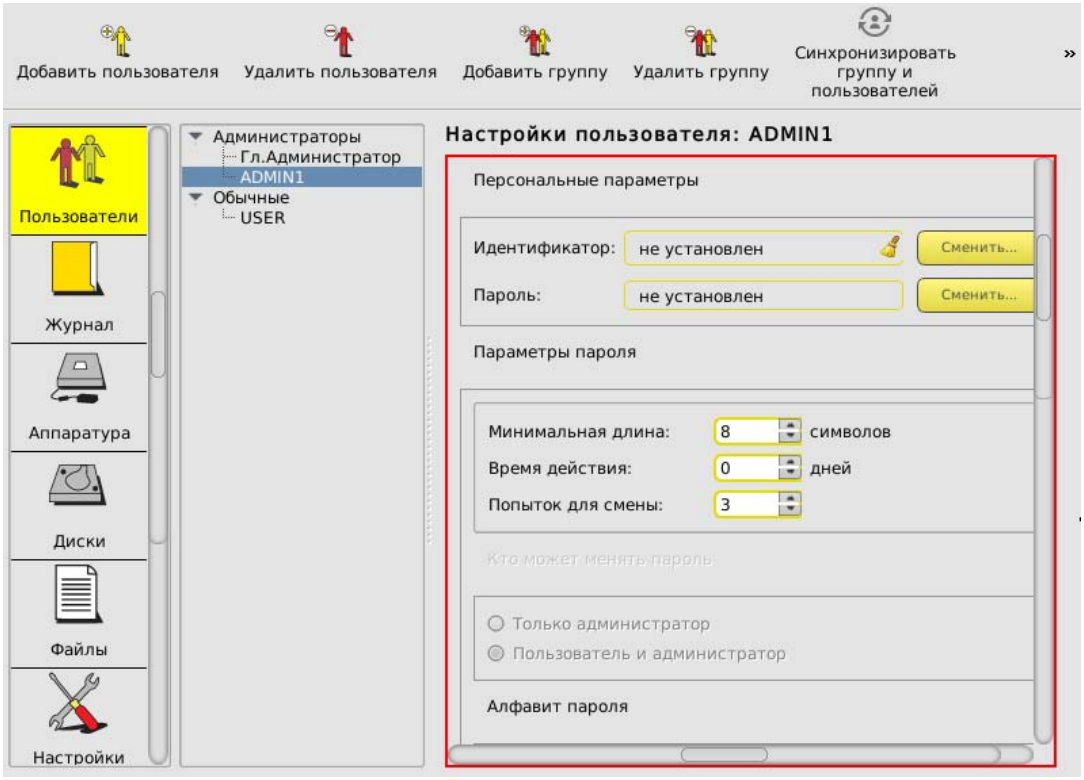

Рисунок 19 – Параметры пользователей в группе «Администраторы» (для моделей МДЗ «Аккорд-МКТ» ТУ 501410-071-37222406-2016, ТУ 501410-082-37222406-2019)

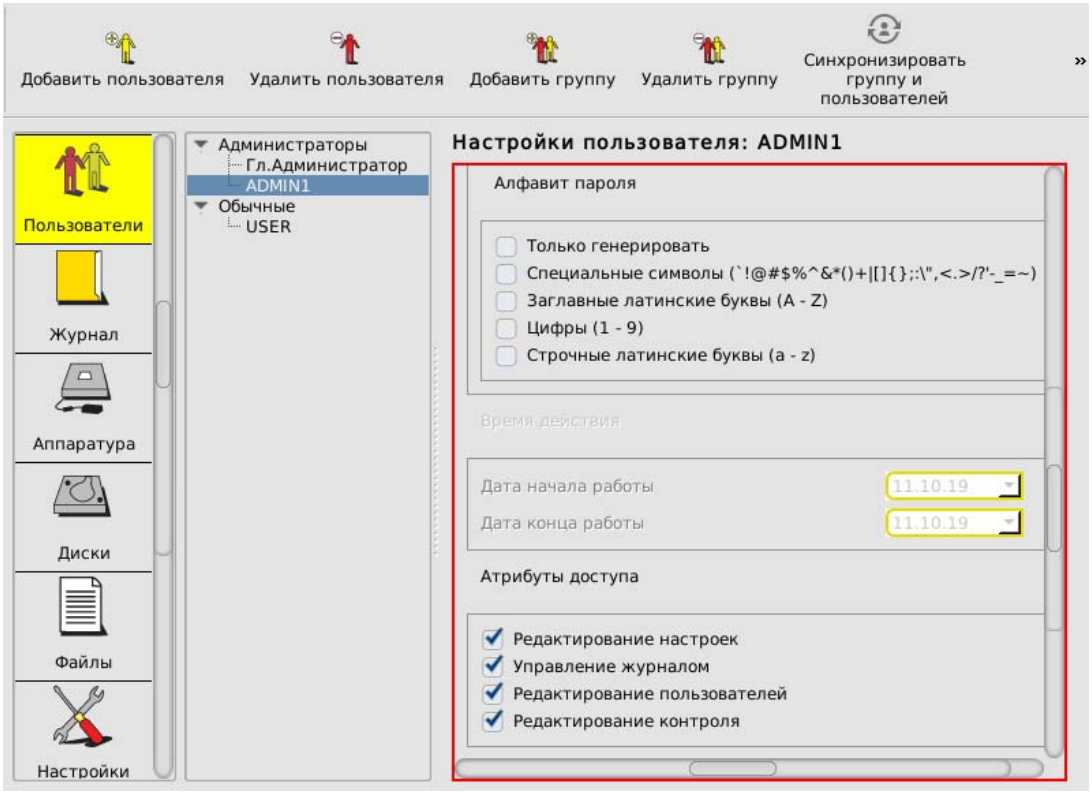

Рисунок 20 - Параметры пользователей в группе «Администраторы» (для моделей МДЗ «Аккорд-МКТ» ТУ 501410-071-37222406-2016, ТУ 501410-082-37222406-2019)

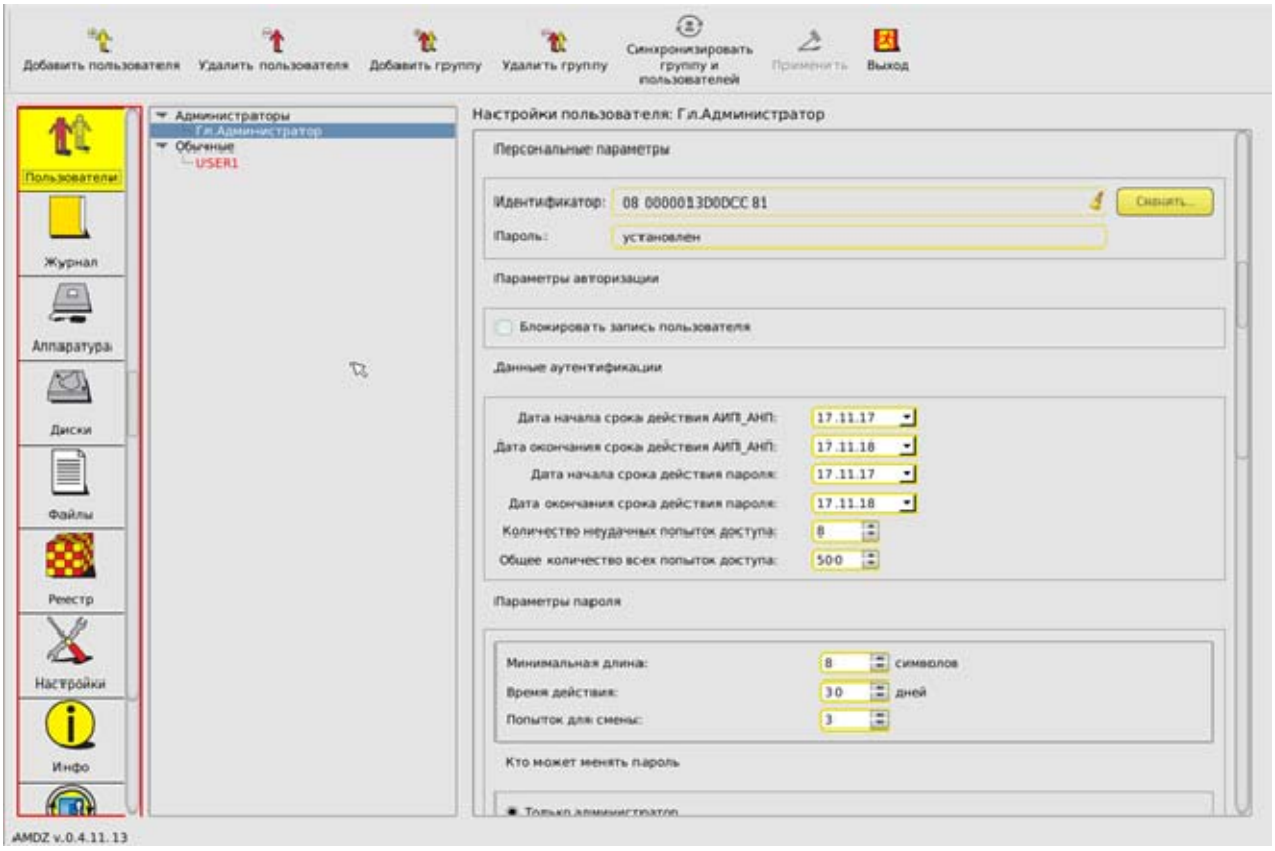

Рисунок 21 - Параметры пользователей в группе «Администраторы» (для модели МДЗ «Аккорд-МКТ» ТУ 501410-112-37222406-2023)

5.3.4.2. Персональные параметры

Каждый пользователь группы «Администраторы» обладает персональными параметрами (рисунок 19):

- идентификатор;
- пароль.

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 5.2.3.

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 5.2.4.

5.3.4.3. 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.

5.3.4.4. Данные аутентификации (ТУ 501410-112-37222406-2023)

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

– является обязательной и может быть выполнена либо на этапе настройки общих параметров группы, либо на этапе настройки каждой учетной записи;

– аналогична процедуре настройке данных аутентификации для учетной записи «Гл. Администратор».

5.3.4.5. Параметры пароля

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

5.3.4.6. Время действия

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

5.3.4.7. 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 Главный Администратор – супервизор (подробнее о супервизоре см. в подразделе 5.2.4) – или любой администратор, обладающий правом редактирования пользователей (т.е. входящий в группу «Администраторы» пользователь, при настройке учетной записи которого в атрибутах доступа установлен флаг «Редактирование пользователей»).

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

- Редактирование настроек. При установке данного флага выбранный пользователь может изменять общие настройки МДЗ «Аккорд-МКТ» (подробнее см. 5.13). 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. 5.12). 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 5.3.2, 5.3.3, 5.3.4, 5.3.5, 5.6, 5.7, 5.8, 5.9). 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 (подробнее см. 5.11). При снятии данного флага для выбранного пользователя функции редактирования списков контроля целостности недоступны, кнопки <Аппаратура>, <Диски> и <Файлы> в меню выбора объектов администрирования неактивны.

5.3.5. Параметры пользователей в группе «Обычные»

Для пользователей группы «Обычные» установлены следующие параметры (рисунок 22 - 24):

– персональные параметры;
– параметры авторизации;
– данные аутентификации (ТУ 501410-112-37222406-2023);
– параметры пароля;
– время действия.

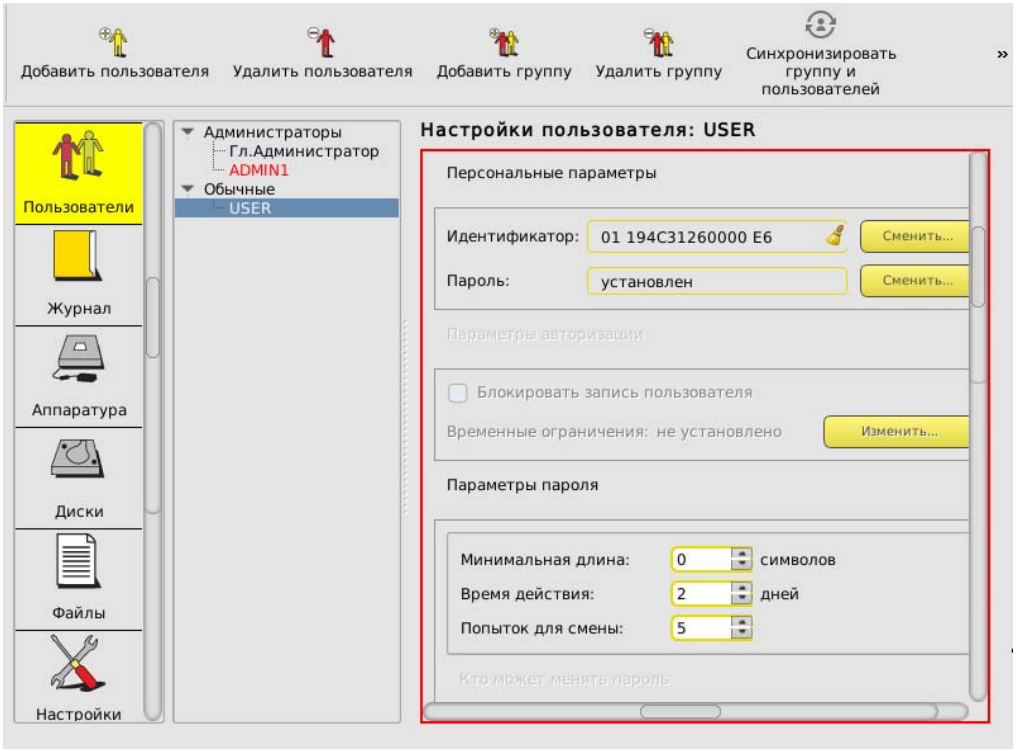

Рисунок 22 – Параметры пользователей в группе «Обычные» (для моделей МДЗ «Аккорд-МКТ» ТУ 501410-071-37222406-2016, ТУ 501410-082-37222406-2019)

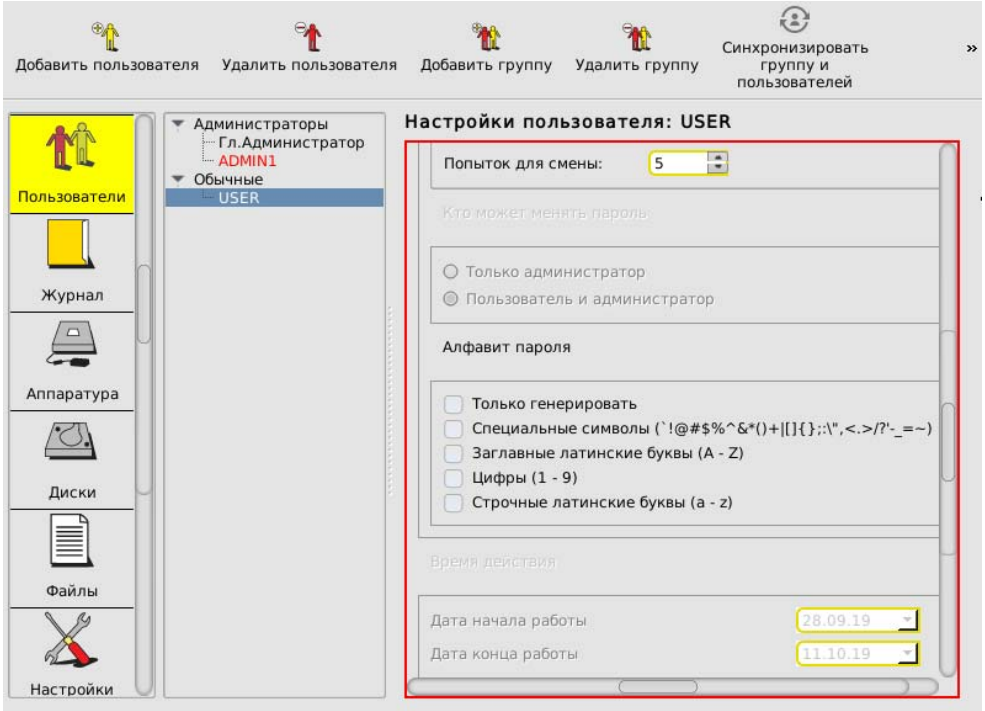

Рисунок 23 - Параметры пользователей в группе «Обычные» (для моделей МДЗ «Аккорд-МКТ» ТУ 501410-071-37222406-2016, ТУ 501410-082-37222406-2019)

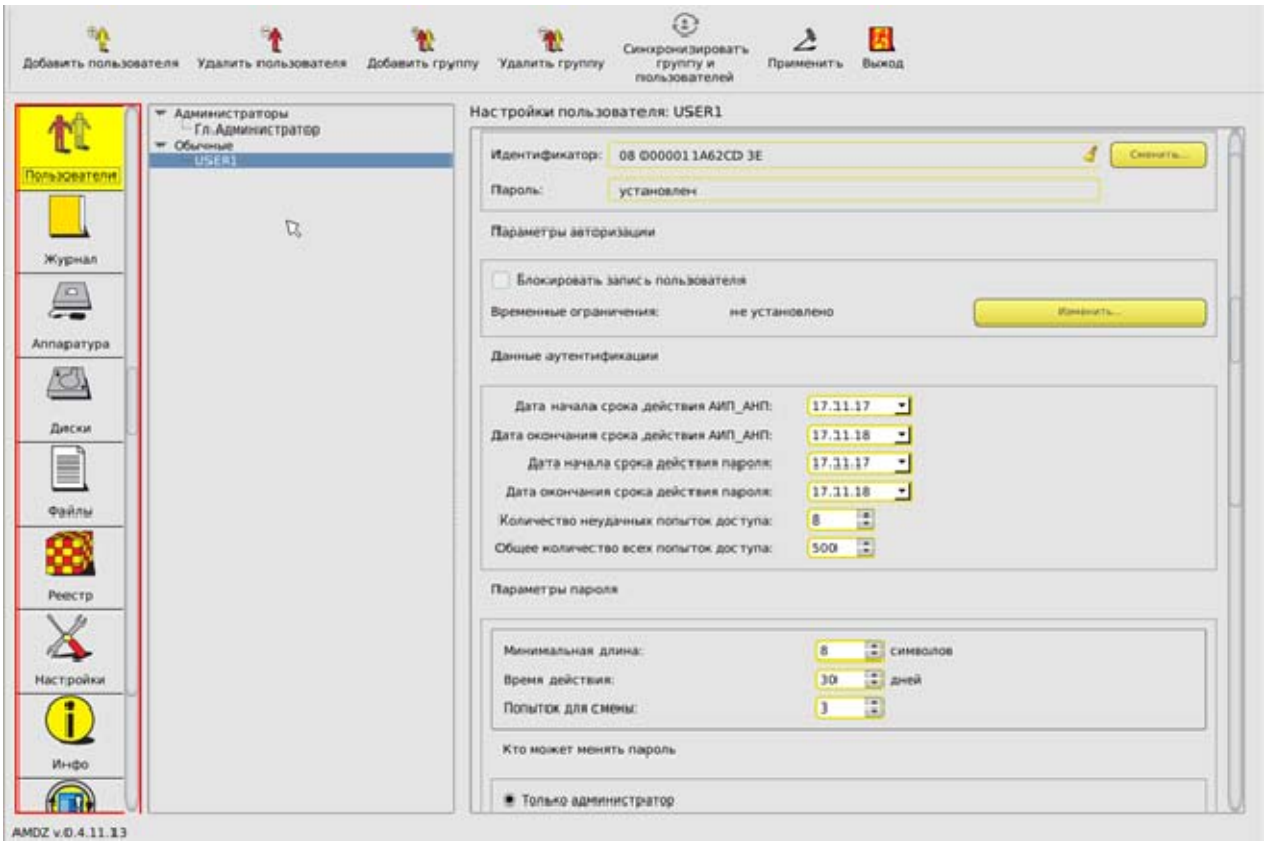

Рисунок 24 - Параметры пользователей в группе «Обычные» (для модели МДЗ «Аккорд-МКТ» ТУ 501410-112-37222406-2023)

5.3.5.1. Персональные параметры

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

5.3.5.2. Параметры авторизации

Для пользователей группы «Обычные» (ТУ 501410-071-37222406-2016) установлены следующие параметры авторизации:

- режим блокировки (см.5.3.5.2.1);
- временные ограничения (см.5.3.5.2.2).

Для блокировки/ограничения доступа пользователя группы «Обычные» к СВТ (ТУ 501410-082-37222406-2019, ТУ 501410-112-37222406-2023) необходимо войти в меню администрирования под учетной записью администратора с правами на редактирование базы данных пользователей и сменить пароль этому пользователю.

5.3.5.2.1. Режим блокировки

Настройки параметров авторизации пользователей группы «Обычные» в части режима блокировки аналогичны настройкам, описанным в п.5.3.4.3.

5.3.5.2.2. 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 25).

Рисунок 25 - Временные ограничения на вход в систему

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

5.3.5.3. Данные аутентификации (ТУ 501410-112-37222406-2023)

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

- является обязательной и может быть выполнена либо на этапе настройки общих параметров группы, либо на этапе настройки каждой учетной записи;
- аналогична процедуре настройке данных аутентификации для учетной записи «Гл. Администратор».

5.3.5.4. Параметры пароля

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

5.3.5.5. Время действия

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

5.4. Особенности регистрации пользователей в МДЗ «Аккорд-МКТ» (ТУ 26.20.40.140-112-37222406-2023)

При регистрации пользователя параметры его учетной записи предполагают необходимость применения случайной числовой последовательности. Для ее генерирования используется датчик случайных чисел (ДСЧ) – в программном или аппаратном исполнении. В работе МДЗ «Аккорд-МКТ» ТУ 26.20.40.140-112-37222406-2023 задействован аппаратный (физический) ДСЧ как обладающий доказанным качеством и подверженный меньшему влиянию косвенных факторов по сравнению с программным ДСЧ.

В качестве физических датчиков случайных чисел (ФДСЧ) могут использоваться USB-устройство «ПИ ШИПКА» (ТУ 26.20.40.140-096-37222406-2021) и USB-устройство «USB-ДСЧ.РКБ» (ТУ 26.12.1-069-37222406-2024). Для возможности использования устройства «ПИ ШИПКА» следует предварительно установить его СПО на СВТ. «USB-ДСЧ.РКБ» не требует дополнительной настройки – устройство поставляется полностью готовым к использованию, причем не только в качестве ФДСЧ, но и в формате аппаратного сторожевого таймера.

Для применения ФДСЧ достаточно подключить его к ЭВМ на этапе смены идентификатора пользователя, до нажатия кнопки <Далее> (рисунок 26).

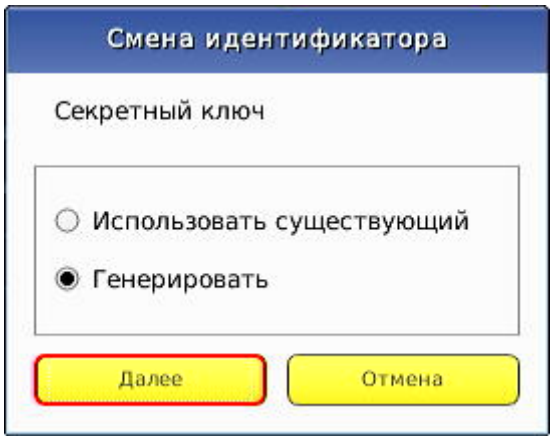

Рисунок 26 – Окно смены идентификатора пользователя

Если в момент нажатия этой кнопки ФДСЧ не будет подключен к ЭВМ, на экране последовательно появятся два информационных сообщения о необходимости провести повторную инициализацию идентификатора (рисунки 27, 28).

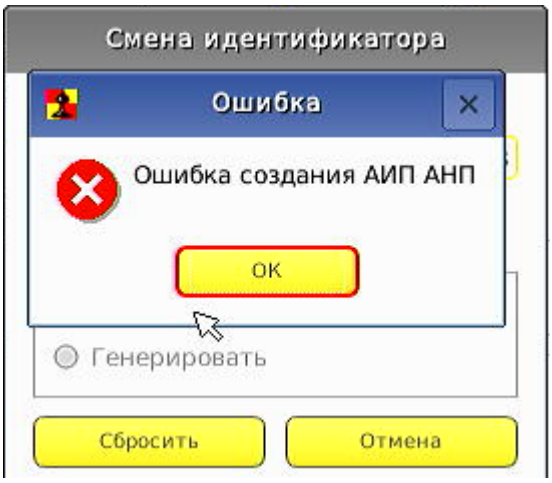

Рисунок 27 – Информационное сообщение в случае, если отсутствует подключение ФДСЧ при попытке смены идентификатора

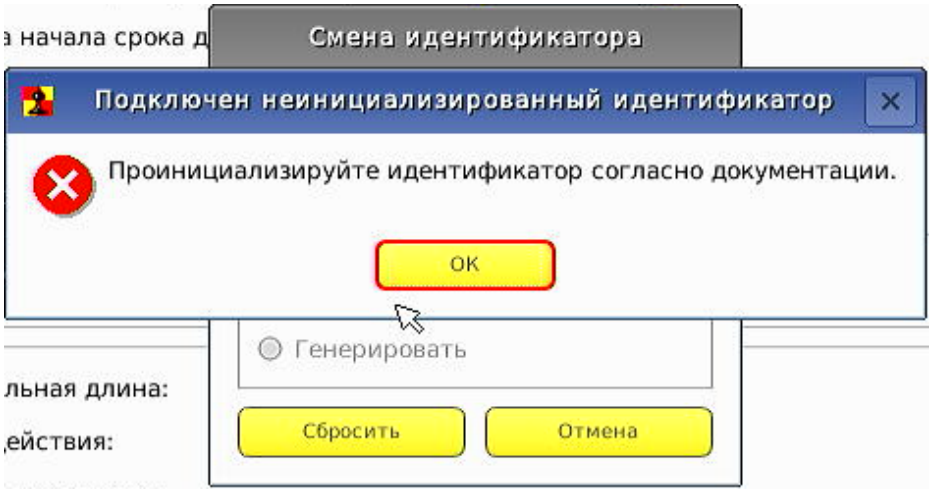

Рисунок 28 – Информационное сообщение о необходимости повторно зарегистрировать идентификатор

При своевременном подключении ФДСЧ регистрация идентификатора проходит успешно (рисунок 29).

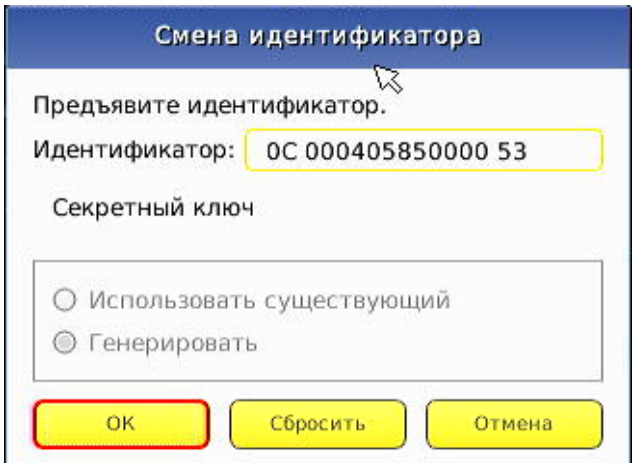

Рисунок 29 – Успешная регистрация идентификатора

5.5. 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 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 Главного Администратора (подробнее см. 5.2).

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

5.6. 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 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 Главного Администратора (подробнее см. 5.2).

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

5.7. Удаление пользователя из списка

Для выполнения процедуры удаления пользователя из списка 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.

5.8. 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 5.3.2 и 5.3.3.

5.9. 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.

5.10. 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.

5.11.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> (ТУ 26.20.40.140-082-37222406-2019, ТУ 26.20.40.140-112-37222406-2023);

– <Диски> (ТУ 26.20.40.140-082-37222406-2019, ТУ 26.20.40.140-112-37222406-2023);

– <Файлы>.

5.11.1. Контроль аппаратуры

«Аккорд-МКТ» 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.

При установке на контроль целостности группы BIOS контролю подлежат следующие разделы BIOS HASH:

– таблицы SMBIOS;
– таблицы ACPI;
– CMOS-память;
– образ BIOS.

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 30, рисунок 31).

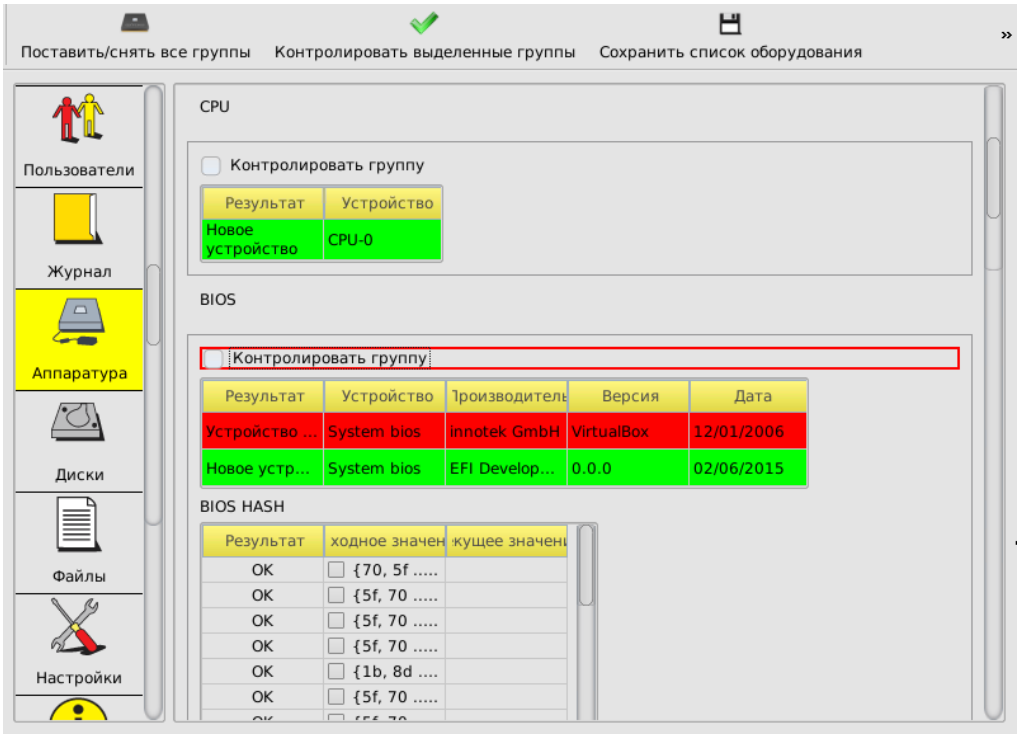

Рисунок 30 - Окно контроля аппаратной части компьютера

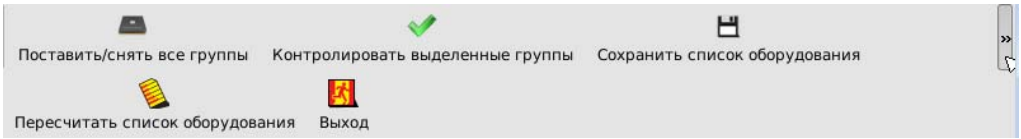

Рисунок 31 - Панель инструментов вкладки «Аппаратура»

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.

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

После регистрации в «Аккорд-МКТ» хотя бы одного пользователя контроль аппаратуры производится при каждой загрузке компьютера после идентификации/аутентификации пользователя. Если обнаруживается несовпадение параметров конфигурации, 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 «Аккорд-МКТ» 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>.

5.11.2. 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 32).

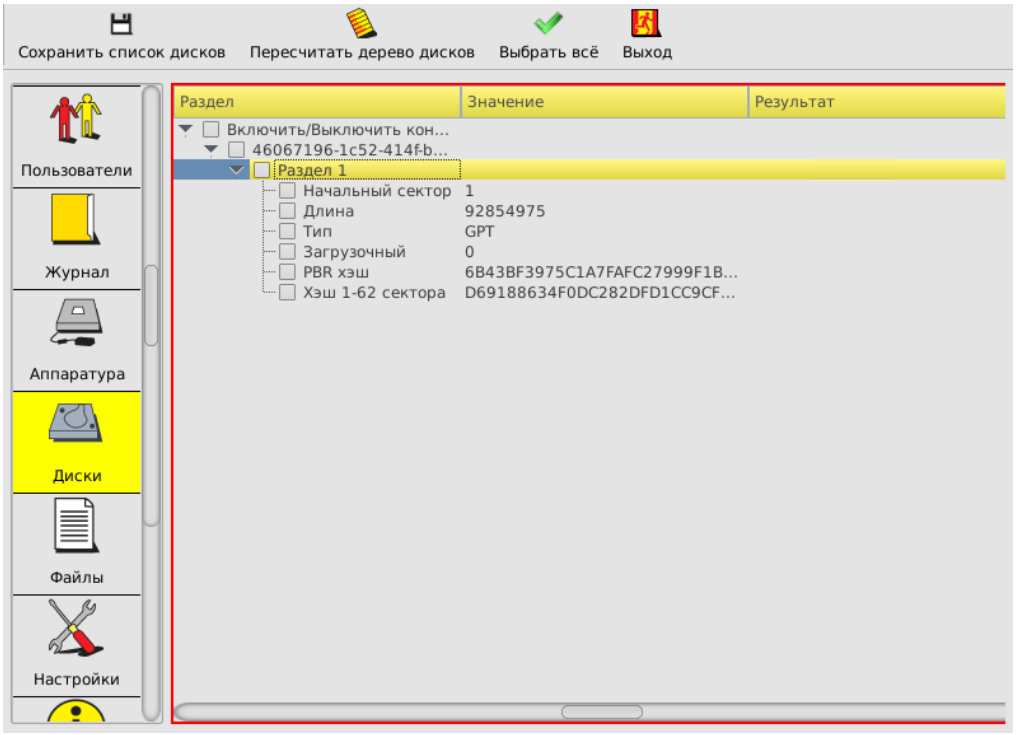

Рисунок 32 - Окно контроля служебных областей диска

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 жестких дисков и других носителей информации (в том числе раздел MBR), независимо от файловой системы. Для записи в память хэш-функций контролируемых областей используется кнопка <Сохранить список оборудования>.

5.11.3. Контроль целостности файлов

Для настройки списков контроля целостности в главном окне среды администрирования нужно выбрать объект администрирования <Файлы>. На экран выводится окно контроля файлов (рисунок 33, рисунок 34).

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

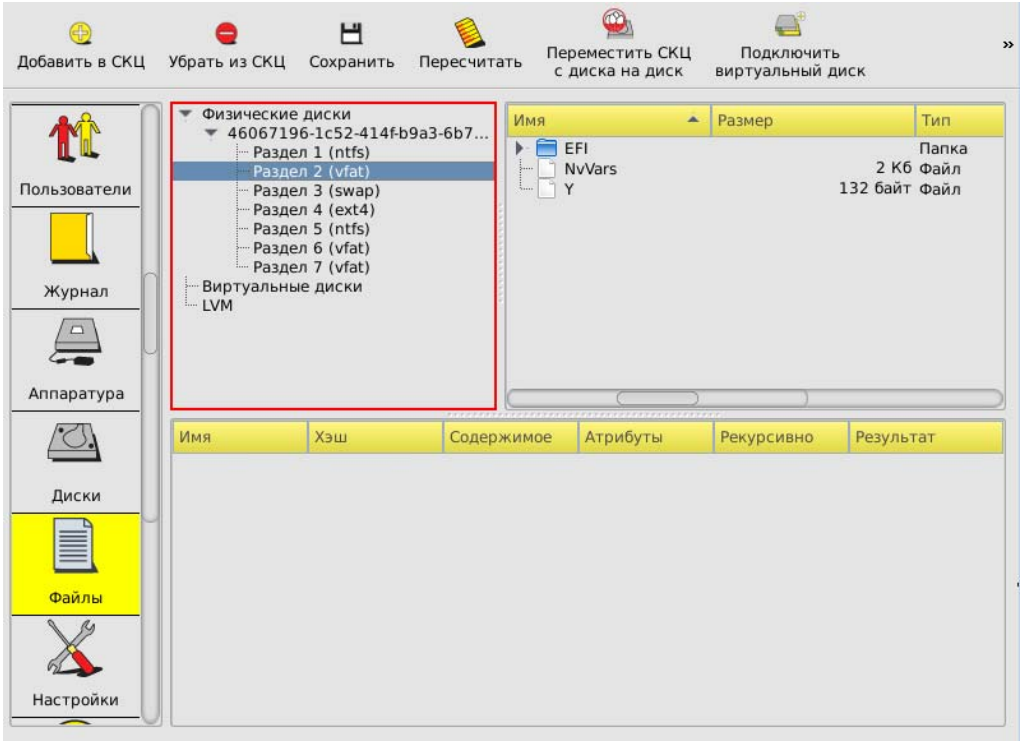

Рисунок 33 - Окно контроля целостности файлов

Рисунок 34 - Панель инструментов окна 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 33);
- 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 35).

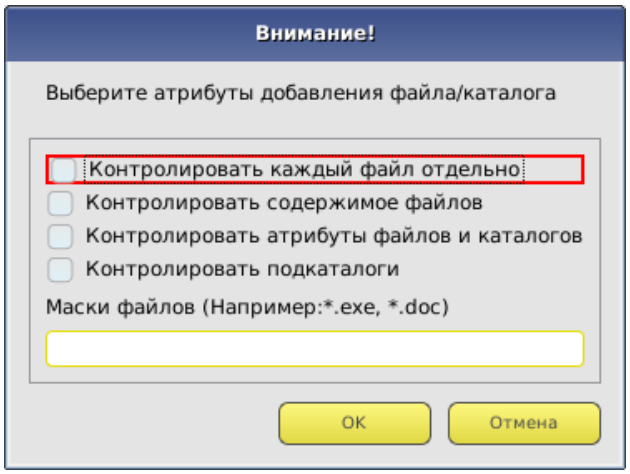

Рисунок 35 – Окно выбора атрибутов добавления каталога

По кнопке <OK> выбранный каталог будет добавлен в список контроля целостности (рисунок 36).

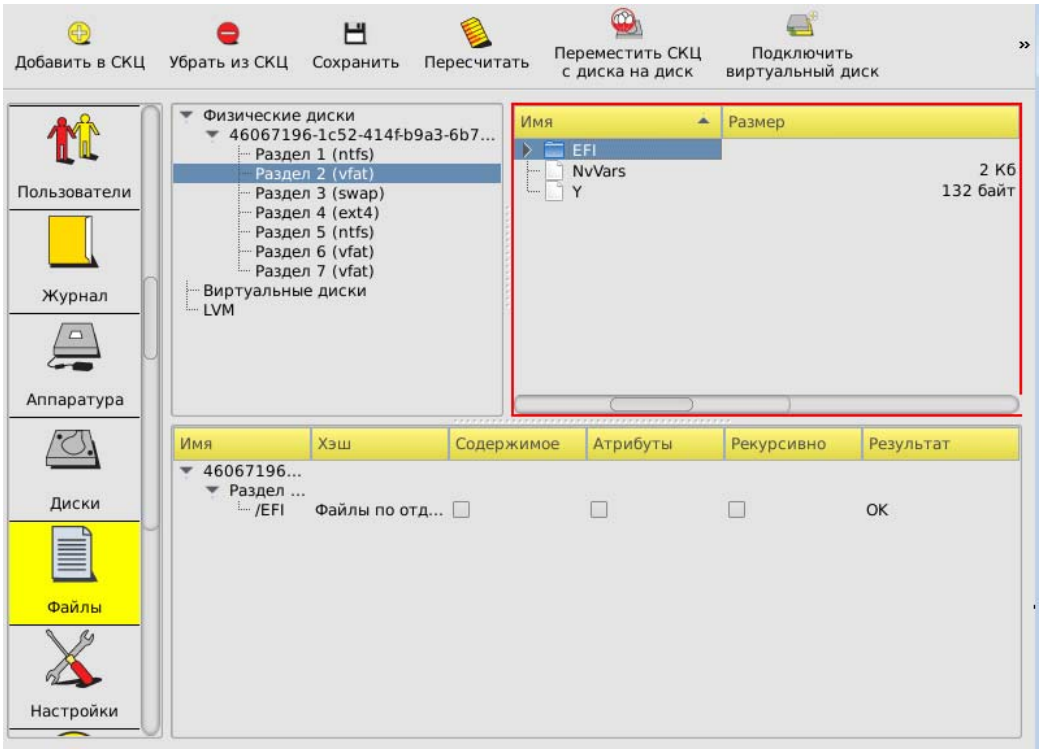

Рисунок 36 – Список контроля целостности с добавленным в него каталогом

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 37).

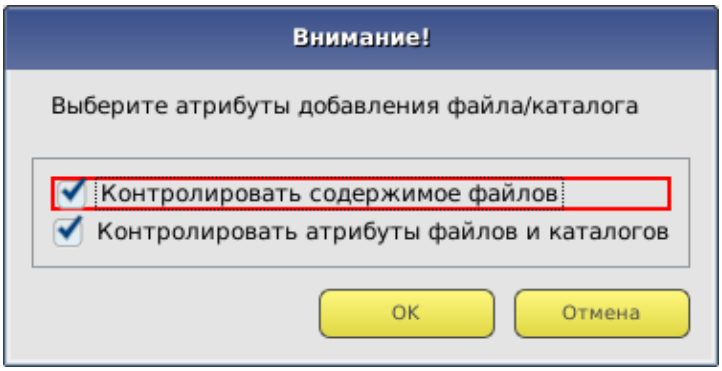

Рисунок 37 – Окно выбора атрибутов добавления файла

По кнопке <OK> выбранный файл будет добавлен в список контроля целостности.

После добавления в список контролируемых файлов всех необходимых файлов и каталогов по кнопке <Сохранить> данные заносятся в память МДЗ «Аккорд-МКТ».

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 «Аккорд-МКТ» и сравнивается с эталонным значением, записанным в памяти МДЗ «Аккорд-МКТ». Если обнаруживается несовпадение, выдается сообщение «Контроль целостности не пройден», и загрузка МДЗ «Аккорд-МКТ» блокируется для обычного пользователя, или выводится стартовое меню, если идентифицирован администратор. При запуске среды администрирования выводится полный список контроля целостности с указанием элементов, не прошедших контроль (рисунок 38).

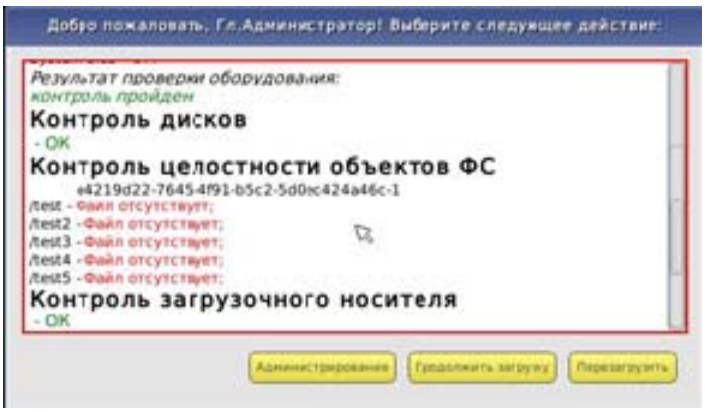

Рисунок 38 – Сообщение о не прошедших контроль целостности элементах

Администратору необходимо изучить содержимое системного журнала (п. 4.11), принять соответствующие меры по выявлению нарушителя, а затем выполнить пересчет контрольных сумм.

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>.

5.11.4. Контроль целостности реестра Windows[3]

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 39).

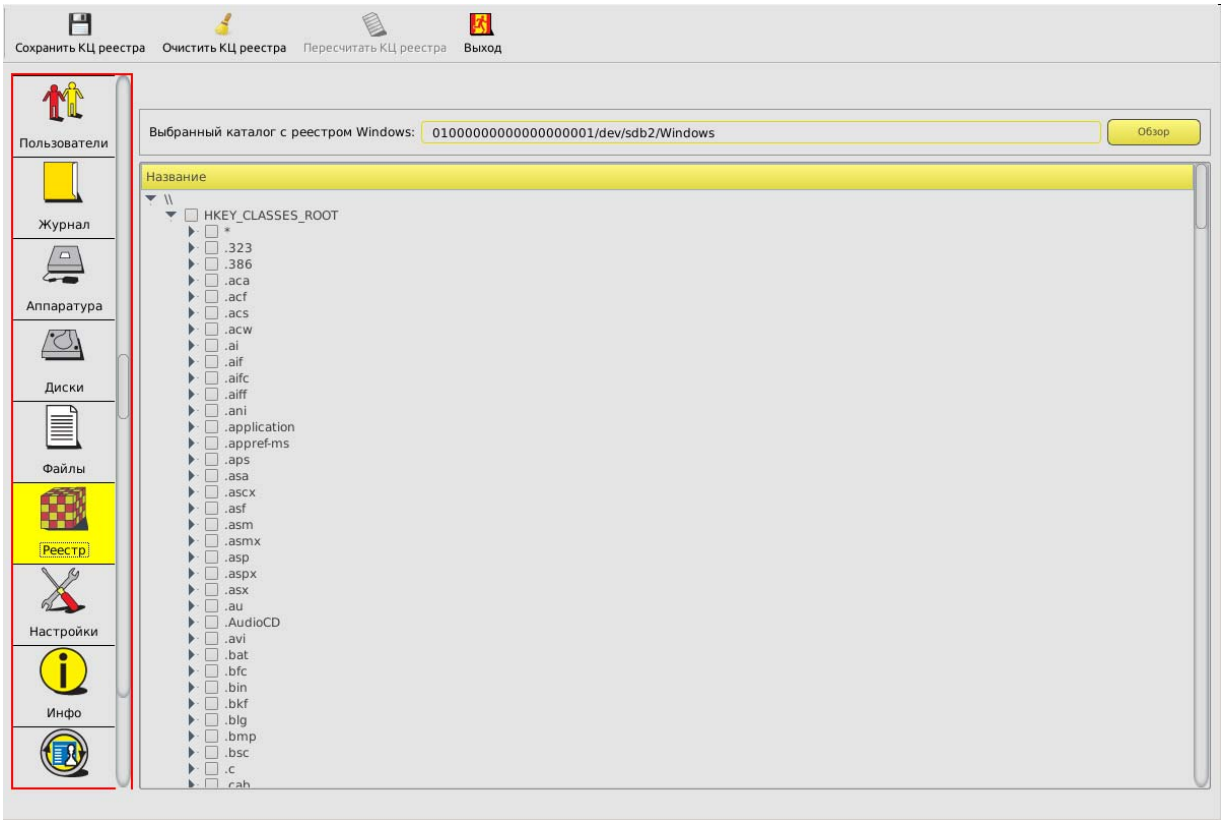

Рисунок 39 - Информация о состоянии реестра

[3] Данная опция поддерживается в МДЗ «Аккорд-МКТ» ТУ 26.20.40.140-112-37222406-2023

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 40).

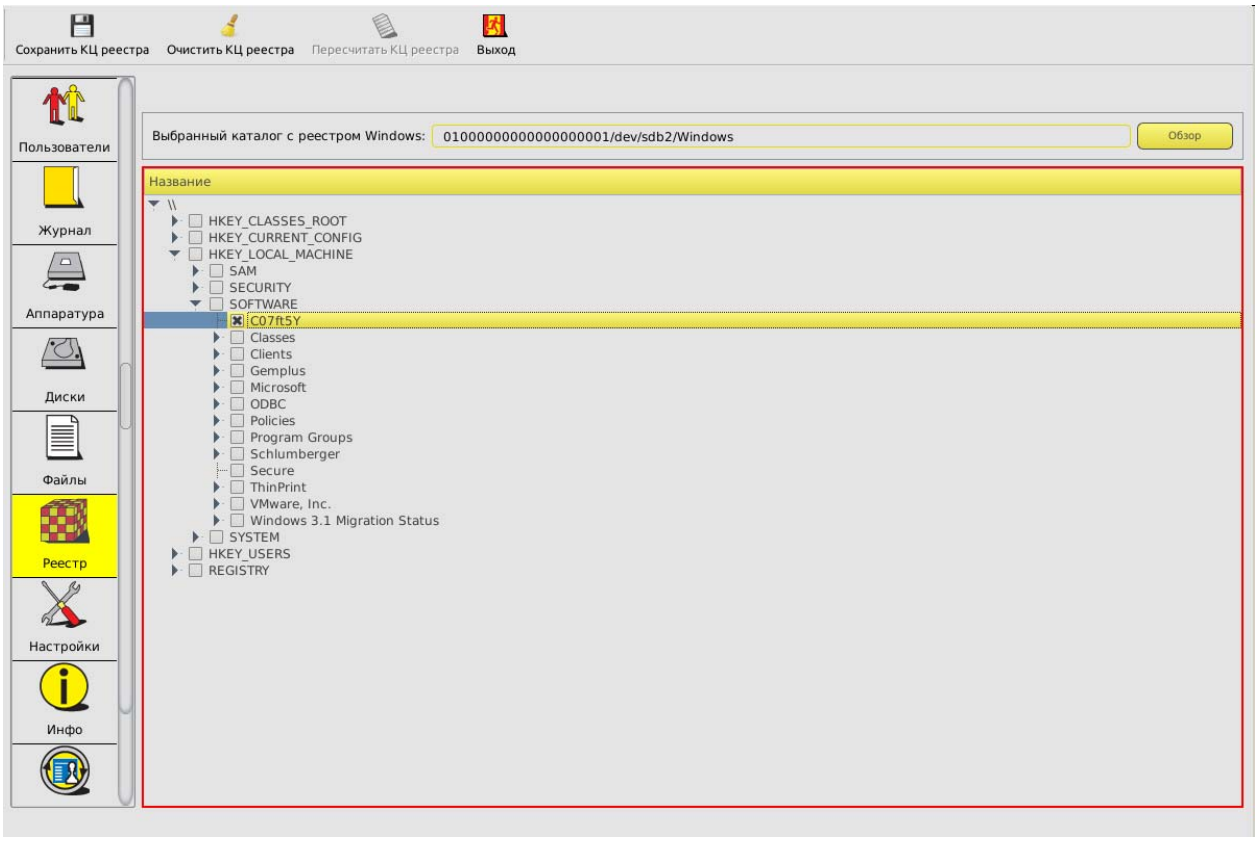

Рисунок 40 - Постановка ветви реестра на контроль целостности

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>.

5.12. Системный журнал

В МДЗ «Аккорд-МКТ» ведется системный журнал. В журнал заносится информация о сеансах работы пользователей с указанием значения идентификатора и всех попытках несанкционированного доступа.

Для просмотра журнала следует в главном окне среды администрирования выбрать объект администрирования <Журнал>. На экран выводится окно системного журнала (рисунок 41).

Для идентификации конкретного пользователя по записи в журнале необходимо найти идентичный указанному в записи TMID среди пользователей на вкладке "Пользователи", после чего с нужной страницы извлечь требующуюся информацию.

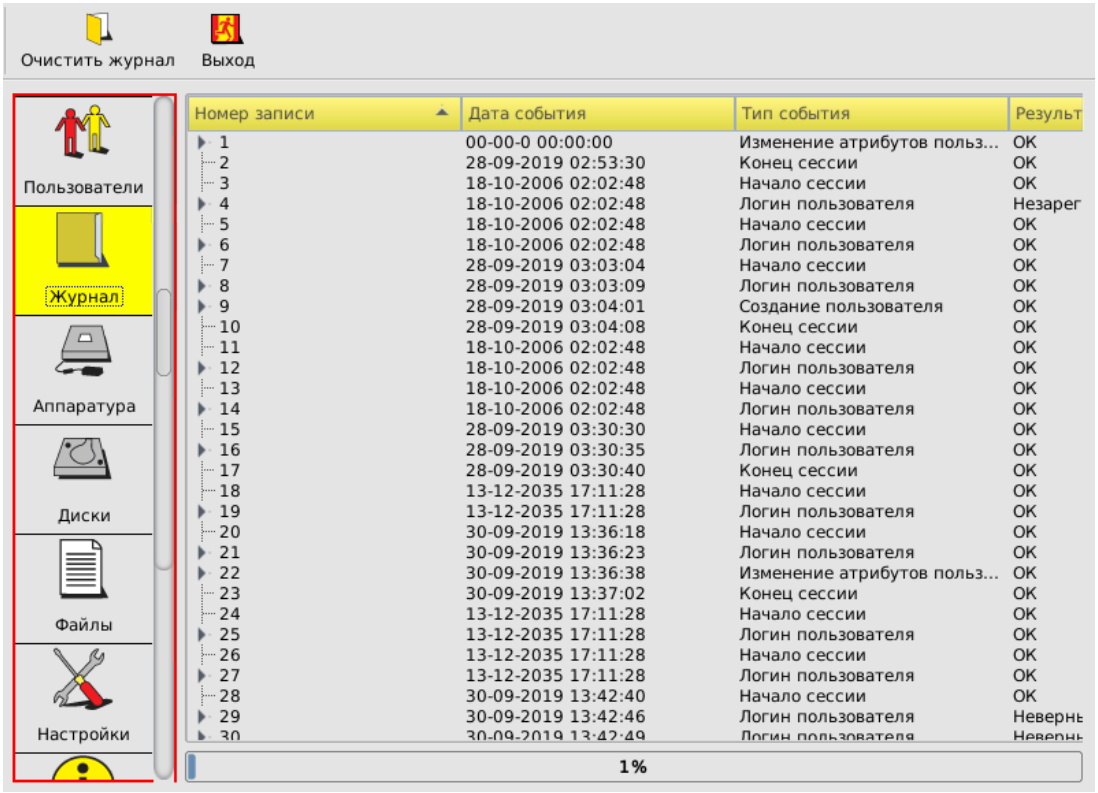

Рисунок 41 - Системный журнал МДЗ «Аккорд-МКТ»

Если заполнение журнала превышает 85%, при загрузке МДЗ «Аккорд-МКТ» 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 41).

5.13.Общие настройки МДЗ «Аккорд-МКТ»

Редактирование общих настроек МДЗ «Аккорд-МКТ» выполняется администратором, обладающим правами на изменение настроек МДЗ «Аккорд-МКТ» (см. п. 5.3.4.7).

Для изменения общих настроек МДЗ «Аккорд-МКТ» необходимо нажать кнопку <Настройки> в меню выбора объектов администрирования. На экран выводится окно с настройками МДЗ «Аккорд-МКТ» (рисунок 42).

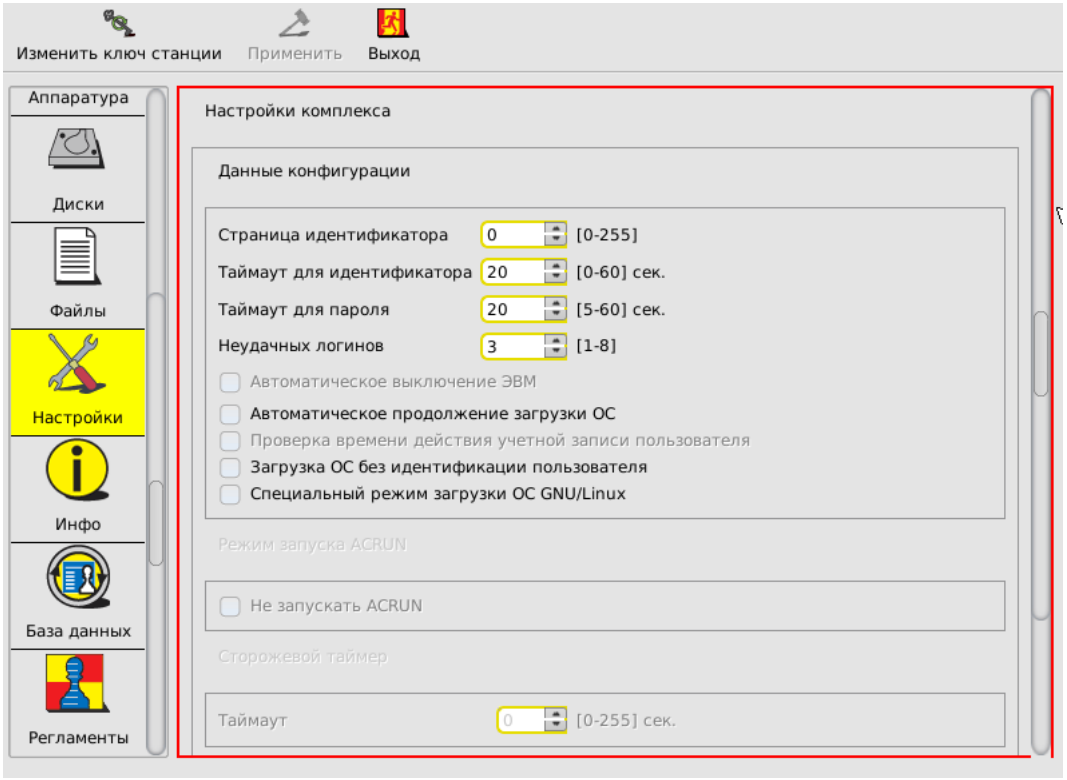

Рисунок 42 – Общие настройки МДЗ «Аккорд-МКТ»

5.13.1. Данные конфигурации

Для настроек данных конфигурации установлены следующие параметры:

- страница идентификатора;
- тайм-аут для идентификатора;
- тайм-аут для пароля;
- количество неудачных логинов;
- автоматическое выключение ЭВМ;
- автоматическое продолжение загрузки ОС;
- проверка времени действия учетной записи пользователя;
- загрузка ОС без идентификации пользователя;
- специальный режим загрузки ОС GNU/Linux.

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

«Тайм-аут для идентификатора» и «Тайм-аут 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 выполнить перезагрузку 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 «Тайм-аут для идентификатора») идентификатор пользователя не был предъявлен, ЭВМ автоматически выключается.

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 «Проверка времени действия учетной записи пользователя» позволяет учитывать настройки параметра «Время действия» для учетных записей пользователей (подробнее о настройке параметра «Время действия» см. 5.3.2.3).

Если в настройках конфигурации установлен параметр «Загрузка ОС без идентификации пользователя», то в процессе загрузки МДЗ «Аккорд-МКТ» выполнение процедур идентификации и аутентификации пользователя не требуется, но загрузка ОС осуществляется только после успешного завершения всех контрольных процедур[4] (установленных в рамках подраздела 5.11).

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

5.13.2. Установка специального режима загрузки ОС GNU/Linux

В МДЗ «Аккорд-МКТ» 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-МКТ» передает управление выбранному ядру ОС, минуя передачу управления дисками.

---

[4] При загрузке ОС возможно появление ошибки, связанной с некорректной работой загрузчика (только для UEFI). Действия администратора в случае возникновения подобной ошибки описаны в Приложении 4 настоящего руководства.

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

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-МКТ». 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.

5.14. Информация о МДЗ «Аккорд-МКТ»

На вкладке «Инфо» главного окна среды администрирования отображается следующая информация о МДЗ «Аккорд-МКТ»:

- версия ПО «Аккорд-МКТ»;
- серийный номер МДЗ «Аккорд-МКТ»;
- контрольные суммы основных компонентов.

5.15. Экспорт/импорт баз данных

5.15.1. Общие сведения

Базу данных «Аккорд-МКТ» можно скопировать на раздел жесткого диска или специальный USB-носитель, а в случае необходимости загрузить эту копию с жесткого диска или специального USB-носителя. Обычный USB-накопитель в случае использования его для выполнения процедур экспорта/импорта списка пользователей нуждается в специальной подготовке.

5.15.2. 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.

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

5.15.3. Экспорт/импорт баз данных

Для того чтобы начать процедуру экспорта/импорта базы данных «Аккорд-МКТ», 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 43).

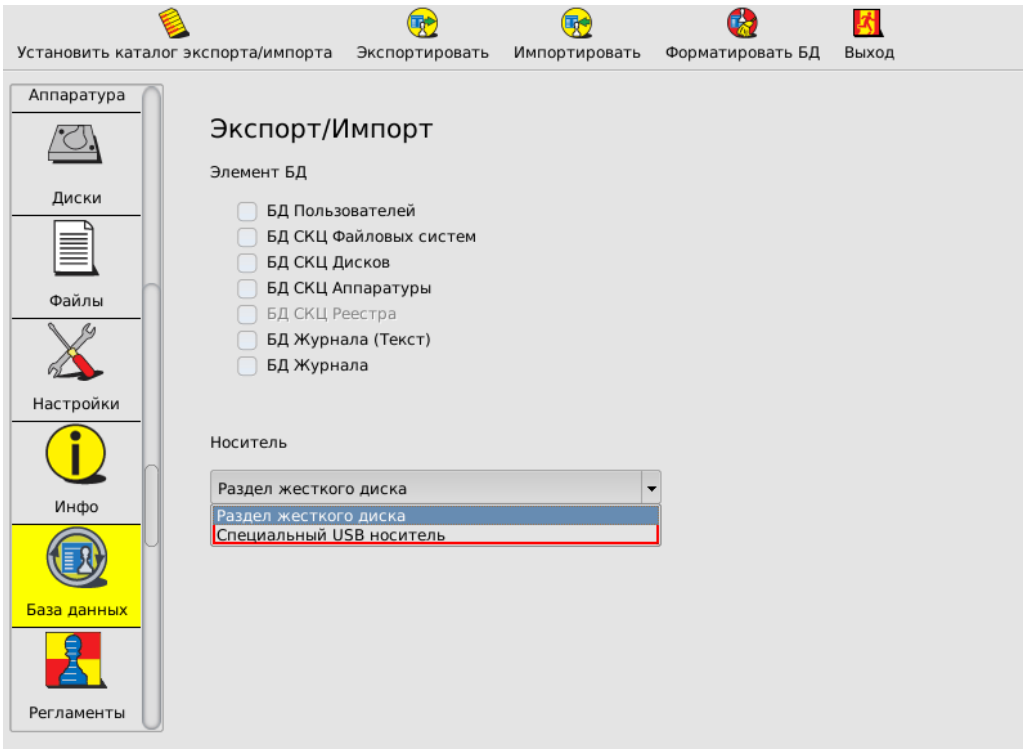

Рисунок 43 - Выбор носителя для экспорта базы пользователей

Далее следует установить каталог экспорта/импорта, нажав на кнопку <Установить каталог экспорта/импорта>, в появившемся окне указав путь к нужной директории и нажав кнопку <OK> (рисунок 44).

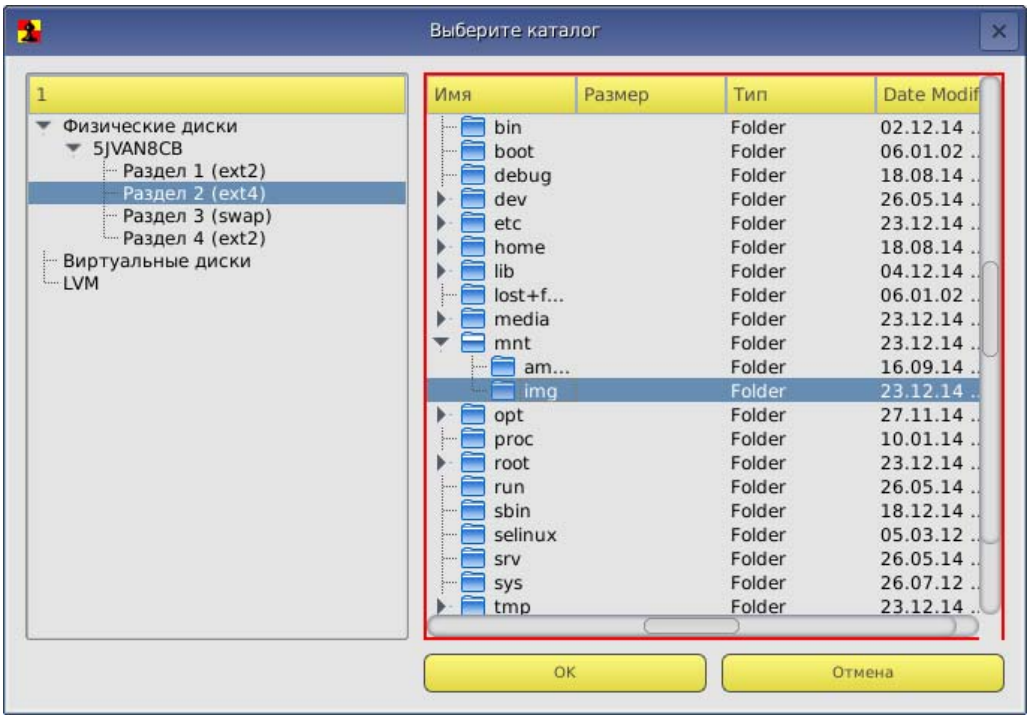

Рисунок 44 - Установка каталога экспорта/импорта БД

После установки каталога экспорта/импорта следует выбрать нужные элементы БД, указав их галочками, и нажать кнопку <Экспортировать>/<Импортировать> (рисунок 43).

ВНИМАНИЕ! Не отключайте специальный USB-носитель сразу после появления сообщения «Данные успешно экспортированы». Для корректного завершения процедуры экспорта БД нужно обязательно выполнить перезагрузку с подключенным USB-носителем! После появления сообщения «Данные успешно импортированы» перезагрузка компьютера выполняется автоматически.

5.15.4. 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.

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

5.15.5. 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 33).

В появившимся окне необходимо указать метку диска от ЭВМ с установленным МДЗ «Аккорд-МКТ», с которой был произведен экспорт, и нажать кнопку <ОК>.

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

Далее следует нажать кнопку <Сохранить> (на верхней панели вкладки «Файлы») и выполнить перезагрузку ЭВМ (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»).

5.16. Форматирование баз данных МДЗ «Аккорд-МКТ»

Процедура форматирования баз данных МДЗ «Аккорд-МКТ», вызываемая кнопкой <Форматировать БД> на вкладке «База данных» главного окна среды администрирования (рисунок 43), позволяет Главному Администратору очистить все внутренние базы данных МДЗ «Аккорд-МКТ», т.е. провести его повторную инициализацию.

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

5.17.Регламентные проверки

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

На вкладке «Регламенты» (рисунок 45) главного окна среды администрирования можно выполнить следующие регламентные проверки в рамках самотестирования «Аккорд-МКТ»:

- проверка ФГСЧ;
- проверка целостности ПО
- проверка целостности данных.

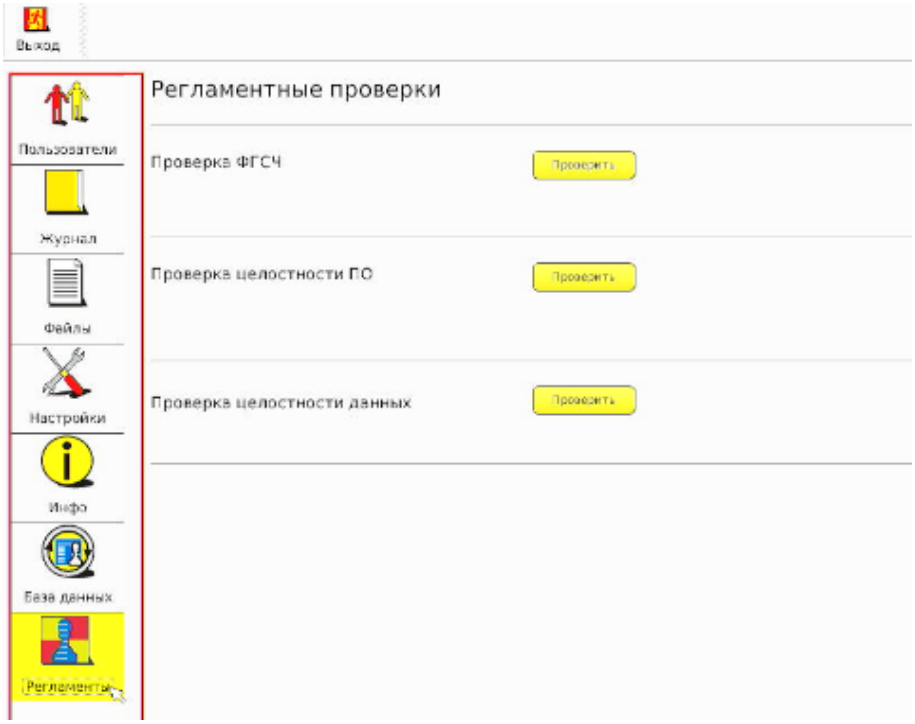

Рисунок 45 – Регламентные проверки

5.18. Выход из среды администрирования

Выход из среды администрирования выполняется при нажатии кнопки <Выход> в главном меню. После этого администратор может или снова войти в среду администрирования, или выполнить перезагрузку компьютера (рисунок 46).

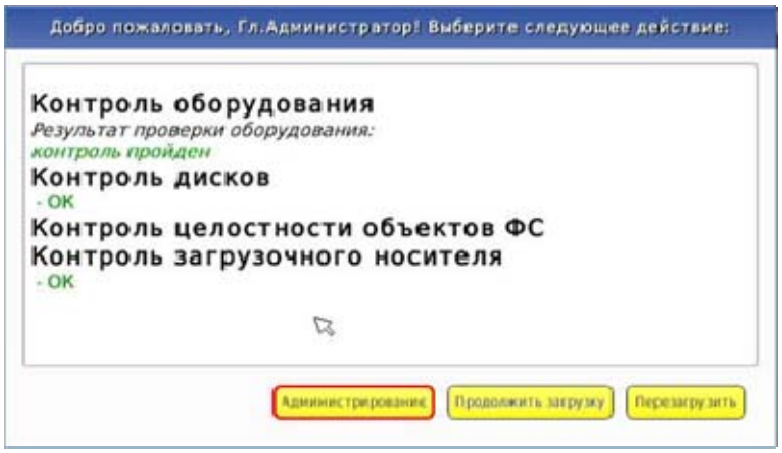

Рисунок 46 - Выход из среды администрирования

После перезагрузки и успешной процедуры И/А появится приветственное окно со следующими возможностями (рисунок 47):

- Войти в среду администрирования (кнопка <Администрирование>);
- Продолжить загрузку в ОС (кнопка <Продолжить загрузку>);
- Перезагрузить компьютер (кнопка <Перезагрузить>).

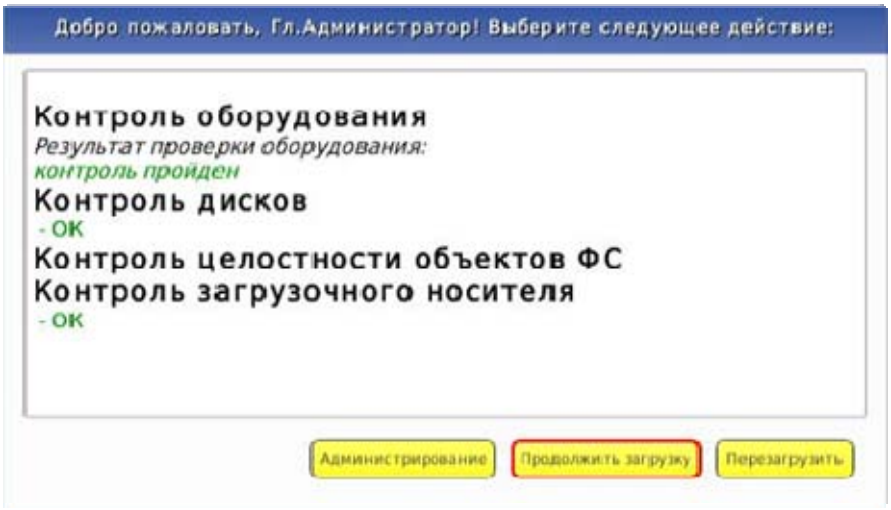

Рисунок 47 - Приветственное окно после процедуры И\А

Следует иметь в виду, что если администратор снова войдет в меню администрирования, кнопка <Продолжить загрузку> станет неактивной до следующей сессии (перезагрузки).

6. Параметры безопасности

Для всех пользователей МДЗ «Аккорд-МКТ» должны быть установлены следующие параметры безопасности:

- парольный механизм аутентификации (установленный пароль и назначенный идентификатор);
- количество неуспешных попыток аутентификации – 3;
- длина пароля до 63 знаков (по умолчанию 8);
- алфавит пароля: специальные символы, заглавные латинские буквы, цифры, строчные латинские буквы.

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

7.1. Требования безопасности к среде ИТ

Представленные в данном подразделе требования реализуются совместно МДЗ «Аккорд-МКТ» и средой информационных технологий (ИТ).

7.1.1. 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 должны реализовывать следующие правила при мониторинге событий, подвергающихся аудиту: накопление или объединение событий по администрированию ОО, событий входов пользователей, событий проверки целостности и редактирования учетных записей пользователей, указывающих на возможное нарушение безопасности.

7.1.2. FIA Идентификация и аутентификация (ТУ 501410-071-37222406-2016)

FIA_UAU.1 Выбор момента аутентификации

FIA_UAU.1.1 ФБ среды функционирования должны запрещать выполнение [список действий отсутствует] 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 должны запрещать выполнение [перечень действий отсутствует] 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.

7.1.3. 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 ФБО.

FPT_STM.1 Надежные метки времени

FPT_STM.1.1 ФБ среды функционирования должны быть способны предоставлять надежные метки времени для собственного использования.

7.2. Указания по выполнению требований безопасности к среде ИТ

Выполнение требований FAU_SAA.1.1 и FAU_SAA.1.2

В МДЗ «Аккорд-МКТ» ведется системный журнал событий (подробнее см. 5.12).

В журнал заносится информация о сеансах работы пользователей с указанием идентификатора и все попытки несанкционированного доступа к ЭВМ.

Перед каждым сеансом работы МДЗ «Аккорд-МКТ» выполняет контроль целостности объектов по спискам контроля.

Если обнаруживается несовпадение параметров конфигурации, записанных в МДЗ «Аккорд-МКТ», и текущих параметров системы, выдается сообщение «Контроль не пройден» и загрузка ЭВМ 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. 5.11).

Выполнение требований FIA_UAU.1 и FIA_UID.1 (ТУ 501410-071-37222406-2016)

Среда функционирования МДЗ «Аккорд-МКТ» 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

МДЗ «Аккорд-МКТ» в процессе каждого старта выполняет ряд тестовых программ для демонстрации правильности выполнения предположений безопасности, обеспечиваемых абстрактной машиной, которая положена в основу МДЗ «Аккорд-МКТ».

Для выполнения данного требования нет необходимости в каких-либо действиях администратора МДЗ «Аккорд-МКТ».

Выполнение требования FPT_STM.1

Среда функционирования МДЗ «Аккорд-МКТ» должна быть способна предоставлять надежные метки времени.

Для выполнения данного требования нет необходимости в каких-либо действиях администратора МДЗ «Аккорд-МКТ».

8. Техническая поддержка

В случае необходимости консультации АО «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) 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
Старт сессии	ОК
Конец сессии	ОК
Логин пользователя	ОК
	Неверный пароль
	Неизвестный идентификатор
	Пользователь заблокирован
	Временные ограничения для пользователя
Создан новый пользователь	ОК
Изменены атрибуты пользователя	ОК
Создана новая группа	ОК
Изменены атрибуты группы	ОК
Модификация СКЦ объектов ФС	ОК
Проверка ДСЧ	ОК
	Неудача
Импорт базы данных	ОК
Экспорт базы данных	ОК
Самотестирование БД пользователей	ОК
	Нарушена
Самотестирование журнала	ОК
	Нарушена
Самотестирование данных КЦ	ОК
	Нарушена
Самотестирование прошивки	ОК
	Нарушена

Приложение 2
Сочетания клавиш, применяемые для работы в среде администрирования «Аккорд-МКТ»

Сочетание клавиш	Описание функциональности	Пояснения
Ctrl+A	Загрузка графического интерфейса	При запросе идентификатора в текстовом интерфейсе (Attach ID:). Не используется в режиме загрузки ОС GNU/Linux
Ctrl+I	Переключение в режим ввода с клавиатуры	При запросе идентификатора в текстовом интерфейсе (Attach ID:). Не используется в режиме загрузки ОС GNU/Linux
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
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
Сценарии загрузки СВТ с установленным МДЗ «Аккорд-МКТ» 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-МКТ» 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. Загрузка продолжится с USB-носителя.

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-МКТ» 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.

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-МКТ» 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. Загрузка продолжится с USB-носителя.

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-МКТ» 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. Загрузка продолжится с USB-носителя.

Приложение 4
Инструкция по настройке загрузчика ОС для обеспечения загрузки в ОС пользователя МДЗ «Аккорд-МКТ»

Современные материнские платы в основном работают на прошивке BIOS типа UEFI. Загрузка в UEFI происходит согласно загрузочным записям.

Каждая загрузочная запись может указывать либо просто на диск, в котором содержится соответствующий FAT-раздел, либо на конкретный .efi файл. В первом случае UEFI будет искать загрузочный файл по умолчанию – у всех операционных систем, установленных в режиме совместимости с UEFI архитектуры x86_64, стартовый образ загрузчика находится в списке загрузочных устройств по пути \EFI\Boot\Bootx64.efi. Пример подобной записи представлен на рисунке 48.

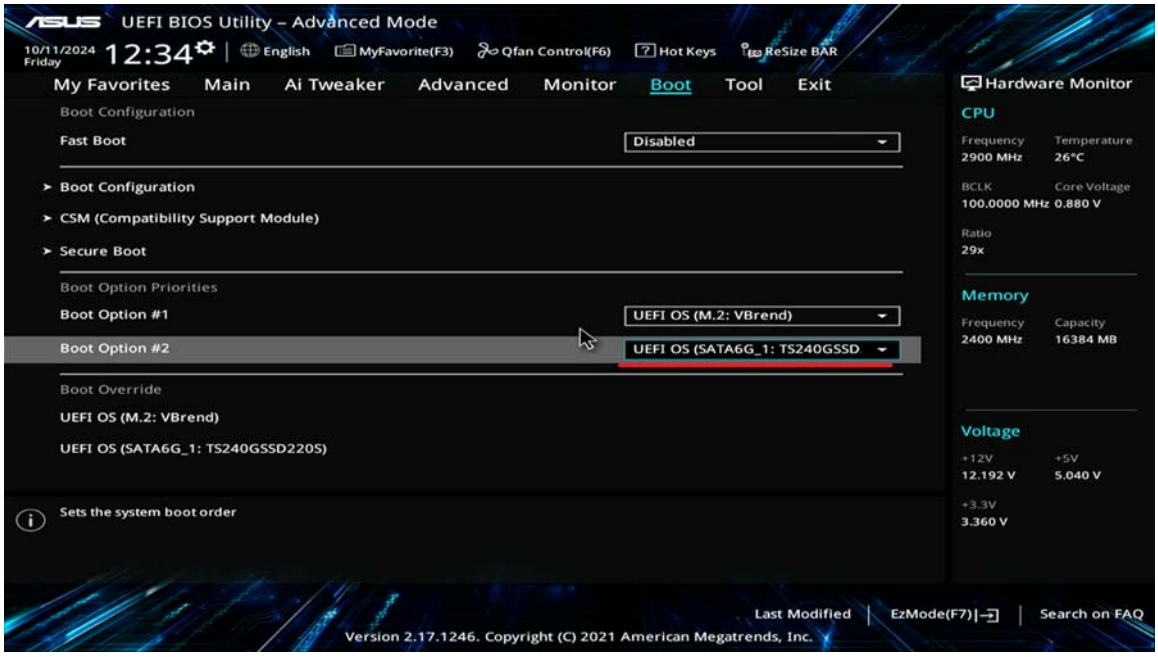

Рисунок 48 - Имя загрузочной записи

При работе с модулями доверенной загрузки производства ОКБ САПР передача управления основному загрузчику операционной системы идет через обращение именно к этому пути (кроме ситуации применения специального режима загрузки ОС GNU\Linux).

В загрузочном списке могут оказаться и другие исполняемые файлы *.efi. Например, производители ОС семейства Linux устанавливают собственный загрузчик UEFI, и путь к нему выглядит так:

\EFI\Имя компании разработчика\grubx64.efi

Пример такой записи представлен на рисунке 49.

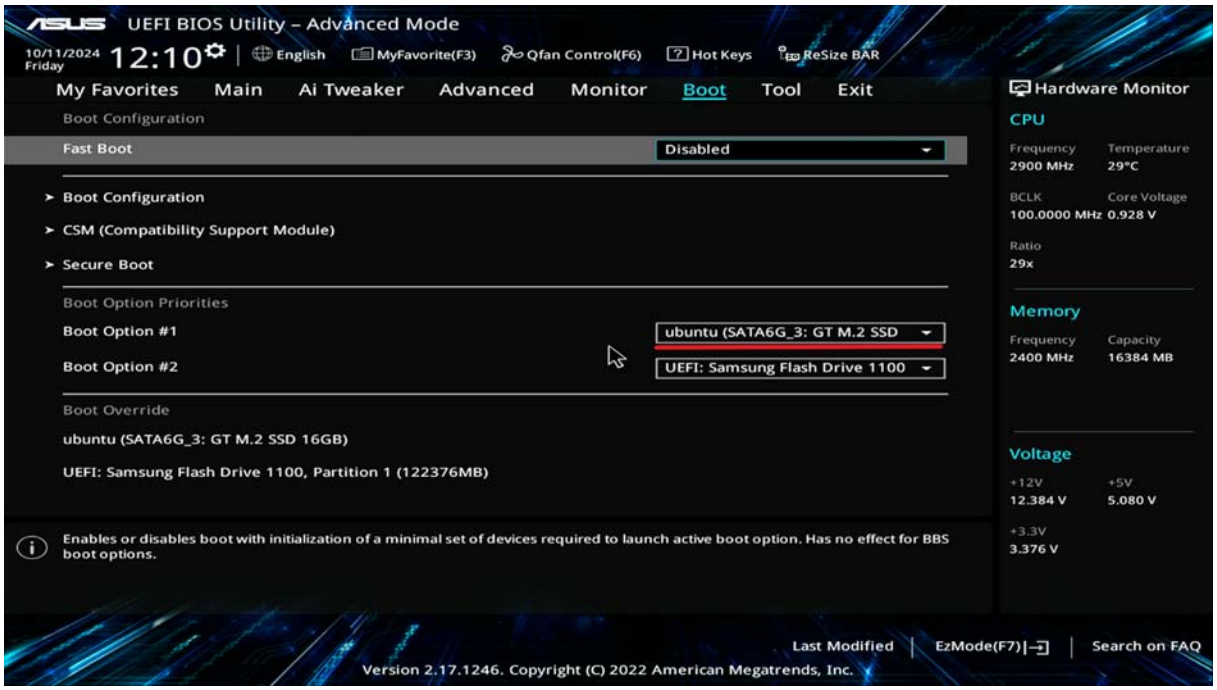

Рисунок 49 - LINUX-загрузчик

При этом стандартный загрузчик тоже есть, но он может не загрузить установленную операционную систему, так как будет являться своеобразной заглушкой.

Для того, чтобы произошла загрузка в доверенную операционную систему, исполняемый файл .efi, загружающий ядро ОС, должен находиться строго по пути \EFI\Boot\Bootx64.efi. В противном случае произойдет инцидент безопасности, который будет сопровождаться сообщением «AMDZ. Bootloader check failed» (рисунки 52-51).

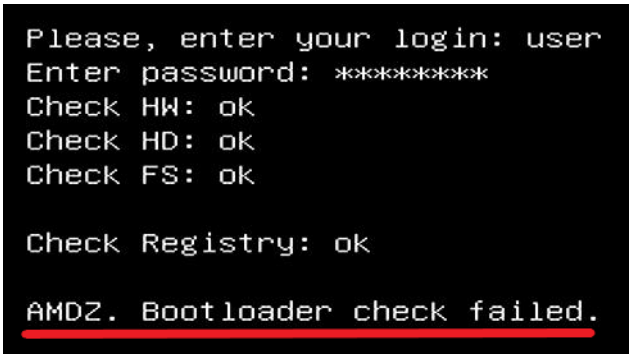

Рисунок 50 - Ошибка при И/А клавиатурным вводом

Рисунок 51 - Ошибка при И/А аппаратным идентификатором

Ниже приведены рекомендации, как можно конфигурировать загрузочный список для восстановления стандартного загрузчика ОС с помощью командной оболочки UEFI Shell.

1. Действия администратора в случае, когда после процедуры идентификации/аутентификации пользователем из группы «Обычные» компьютер перезагружается

Последовательность действий представлена для ОС Ubuntu, поэтому следует учитывать, что названия каталогов для других ОС могут отличаться.

1. Загрузиться в Shell.

2. В списке **Mapping table** найти FSX: загрузочного раздела (X – номер раздела списка, например, FS1: - загрузочный раздел 1).

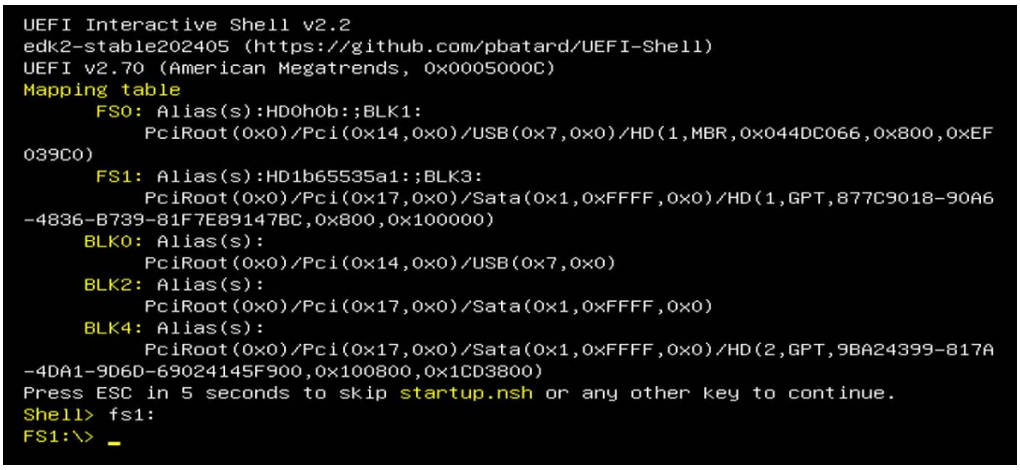

Рисунок 52 - Загрузочный раздел

3. Для просмотра содержимого раздела использовать команду *ls*:

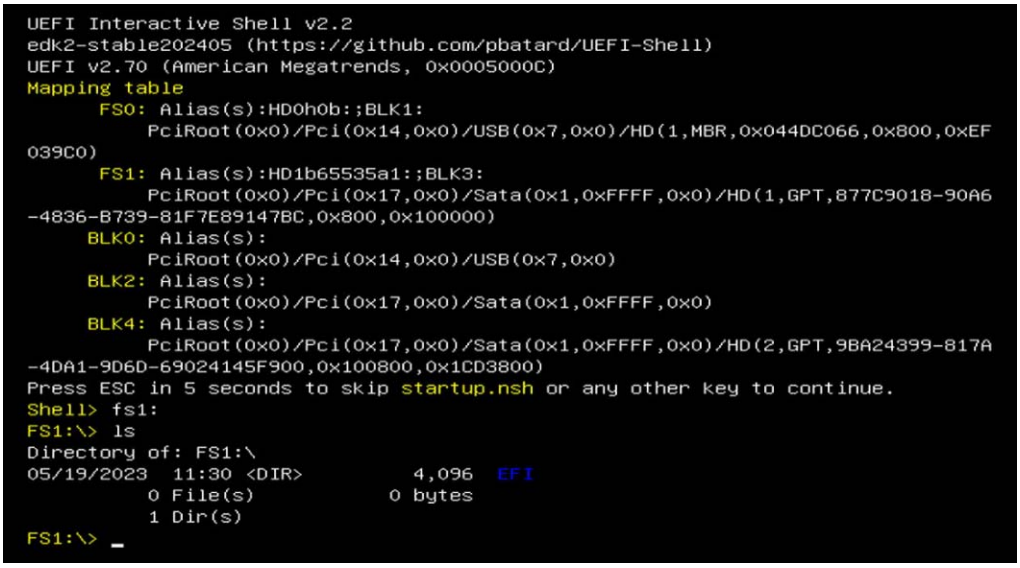

Рисунок 53 - Просмотр содержимого загрузочного раздела

4. Найдя каталог **EFI**, перейти в него командой *cd EFI* и просмотреть его содержимое командой *ls*:

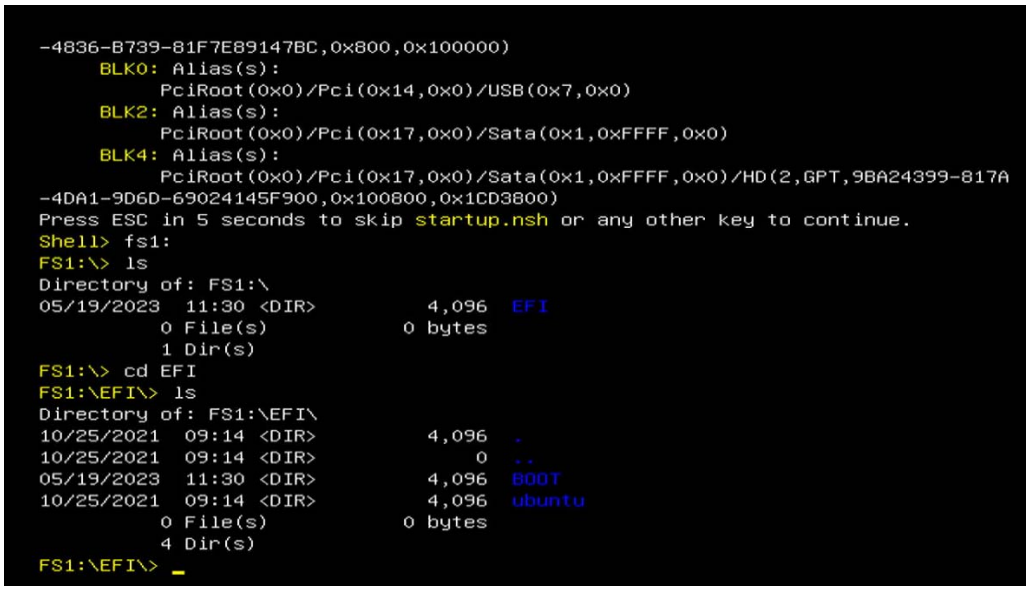

Рисунок 54 - Просмотр содержимого каталога EFI

5. Если в каталоге обнаружатся два подкаталога – BOOT и ubuntu – можно сделать вывод, что раздел найден верно, и перейти к следующему шагу. В противном случае следует повторить шаг 2.

6. Перейти в каталог BOOT и запустить файл bootx64.efi:

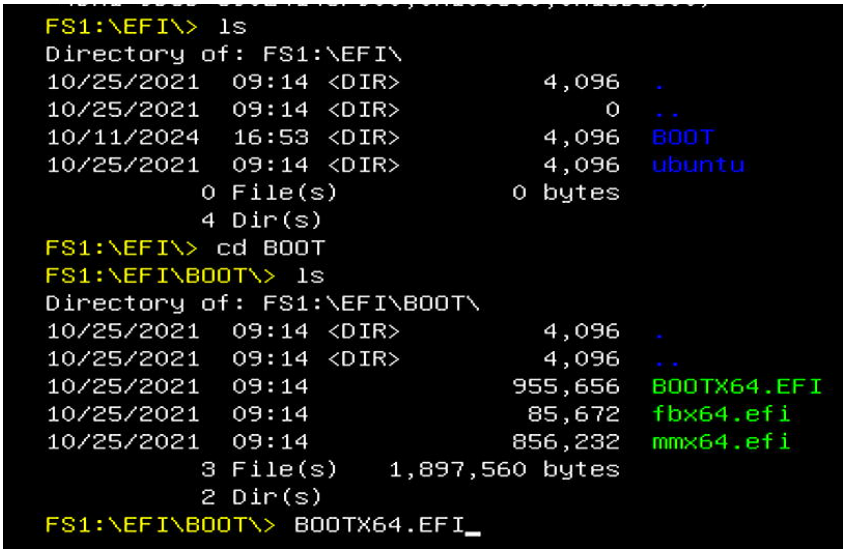

Рисунок 55 - Запуск файла bootx64.efi

7. В случае перезагрузки компьютера на этом этапе повторить действия до шага 5 и далее продолжить их с шага 8.

8. Перейти в каталог ubuntu (команда *cd ubuntu*) и скопировать файл grubx64.efi в каталог EFI\BOOT командой *cp grubx64.efi FS1:\EFI\BOOT*:

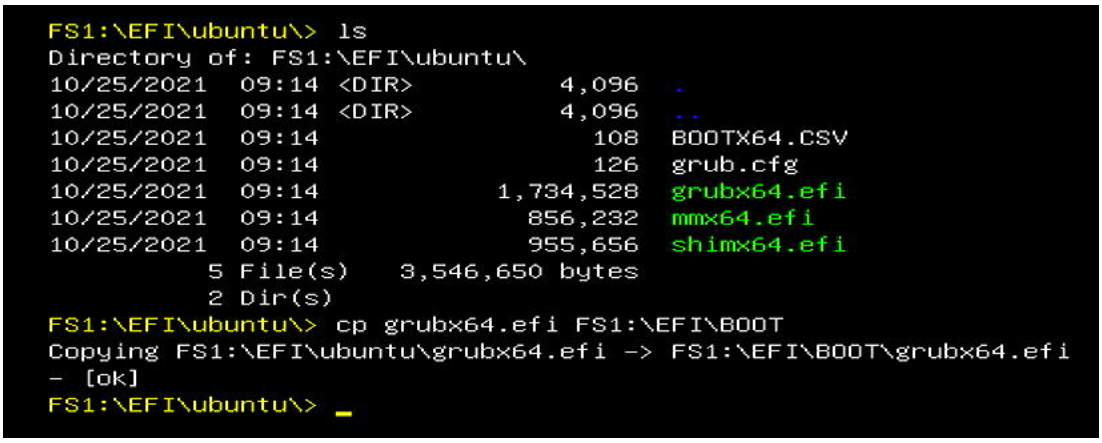

Рисунок 56 - Перемещение файла grubx64.efi в каталог EFI\BOOT

9. Перейти в каталог BOOT по пути **\EFI\BOOT** и переименовать прежний bootx64.efi в любое имя – например, bootx64.efi_old, а перемещенный файл grubx64.efi – в bootx64.efi.

В итоге должен получиться путь **\EFI\Boot\bootx64.efi**.

Команды (рисунок 57):

- *mv bootx64.efi bootx64.efi_old* - переименование прежнего bootx64.efi
- *mv grubx64.efi bootx64.efi* - переименование перемещенного файла grubx64.efi

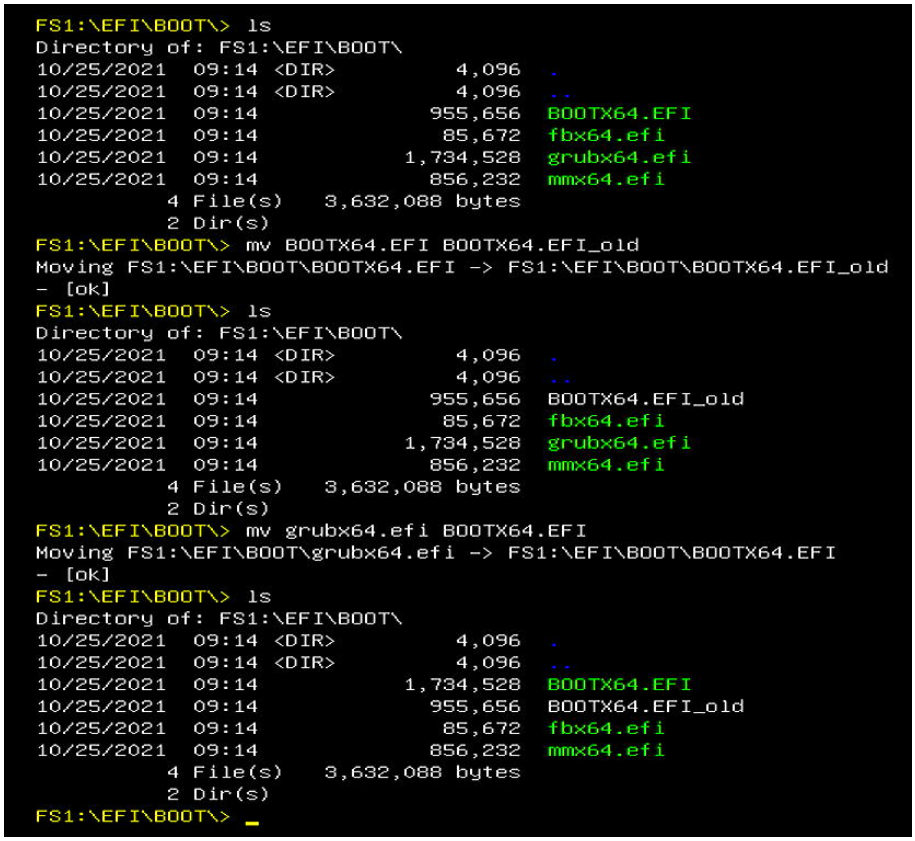

Рисунок 57 - Переименование файлов на шаге 9

10. Проверить продолжение загрузки в операционную систему.

2. Действия администратора в случае, когда после процедуры идентификации/аутентификации пользователем из группы «Обычные» выдается ошибка «AMDZ. Bootloader check failed»

Последовательность действий представлена для ОС Ubuntu, поэтому следует учитывать, что названия каталогов для других ОС могут отличаться.

1. Загрузиться в Shell.
2. В списке **Mapping table** найти FSX: загрузочного раздела (X – номер раздела списка, например, FS1: - загрузочный раздел 1).

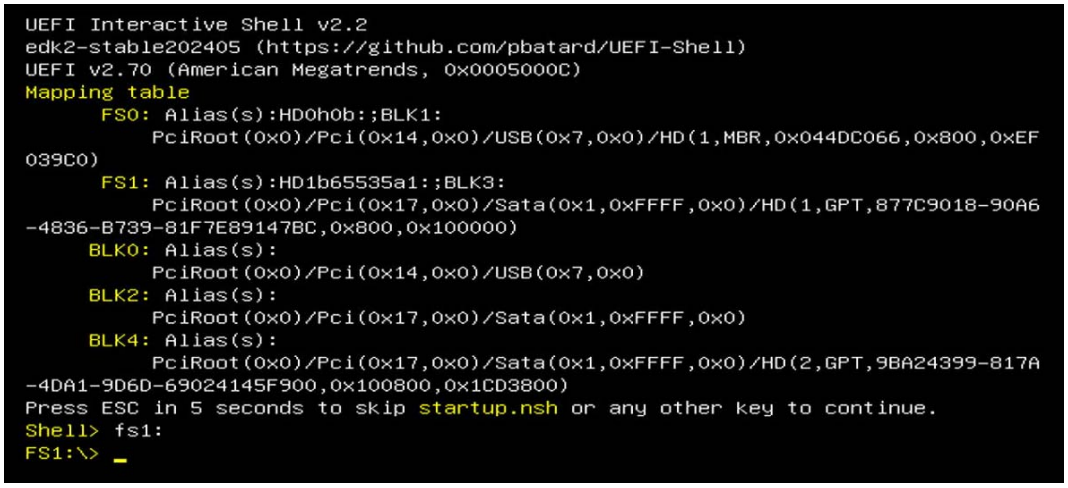

Рисунок 58 - Загрузочный раздел

3. Найдя каталог **EFI**, перейти в него командой *cd EFI* и просмотреть его содержимое командой *ls*:

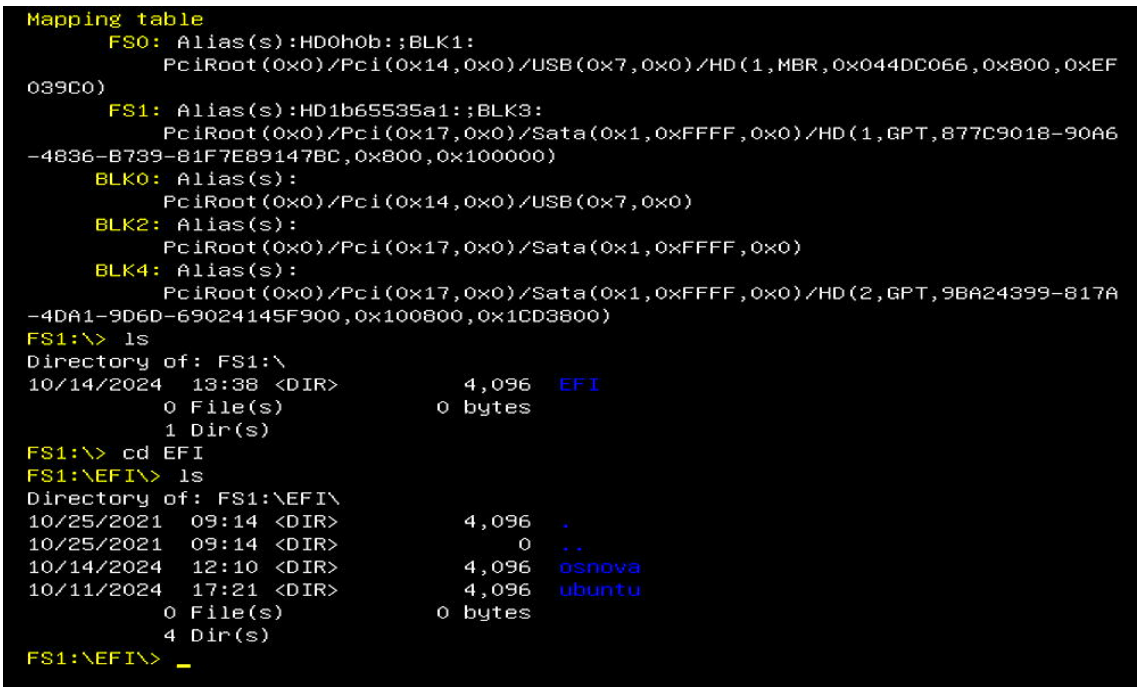

Рисунок 59 - Просмотр содержимого каталога EFI

4. Если вместо подкаталога Boot обнаружится подкаталог с другим именем – например, osnova (рисунок 60) – следует зайти в него и запустить файл bootx64.efi. Если после этого операционная система успешно запустится, то можно перейти к шагу 5 и после шага 6 закончить настройку загрузочного пути.

Если кроме подкаталога ubuntu в каталоге EFI не будет других подкаталогов (рисунок 60), следует перейти к шагу 7.

5. Переименовать подкаталог osnova в BOOT.
6. Проверить продолжение загрузки в операционную систему.
7. В случае отсутствия подкаталога BOOT (рисунок 60) его необходимо создать и заполнить. Создать подкаталог можно командой *mkdir BOOT* (рисунок 61).

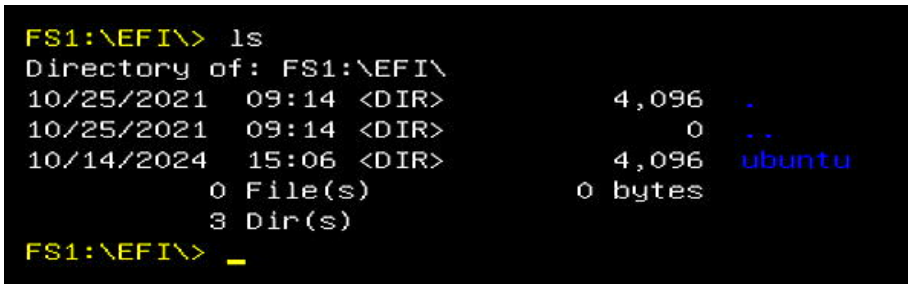

Рисунок 60 - Просмотр содержимого каталога EFI

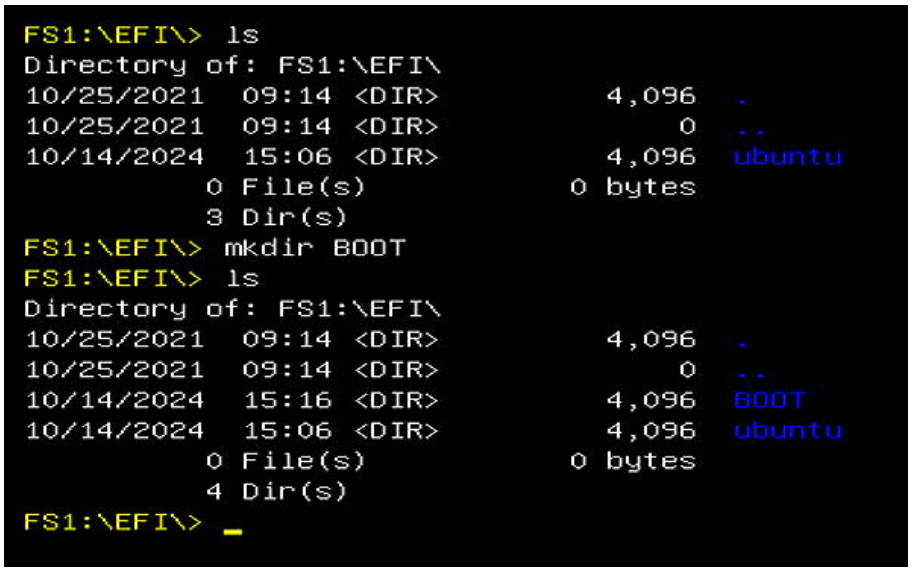

Рисунок 61 - Создание подкаталога BOOT

8. После создания BOOT необходимо положить в него загрузочный файл операционной системы. Для этого следует пройти в соседний каталог ubuntu (команда *cd ubuntu*) и скопировать файл grubx64.efi с именем bootx64.efi в ранее созданный подкаталог BOOT (команда *cp grubx64.efi FS1:\EFI\BOOT*):

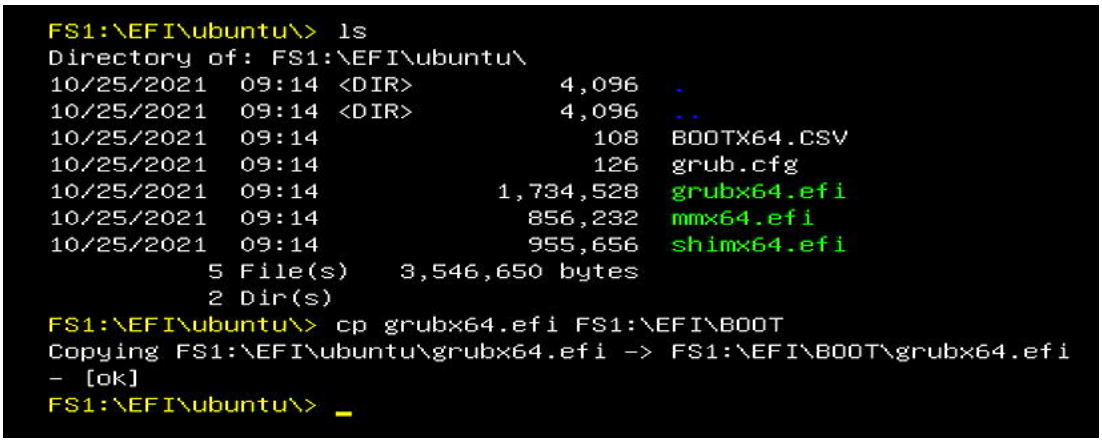

Рисунок 62 - Копирование загрузочного файла в подкаталог BOOT

9. Перейти в каталог BOOT и переименовать скопированный файл grubx64.efi в bootx64.efi:

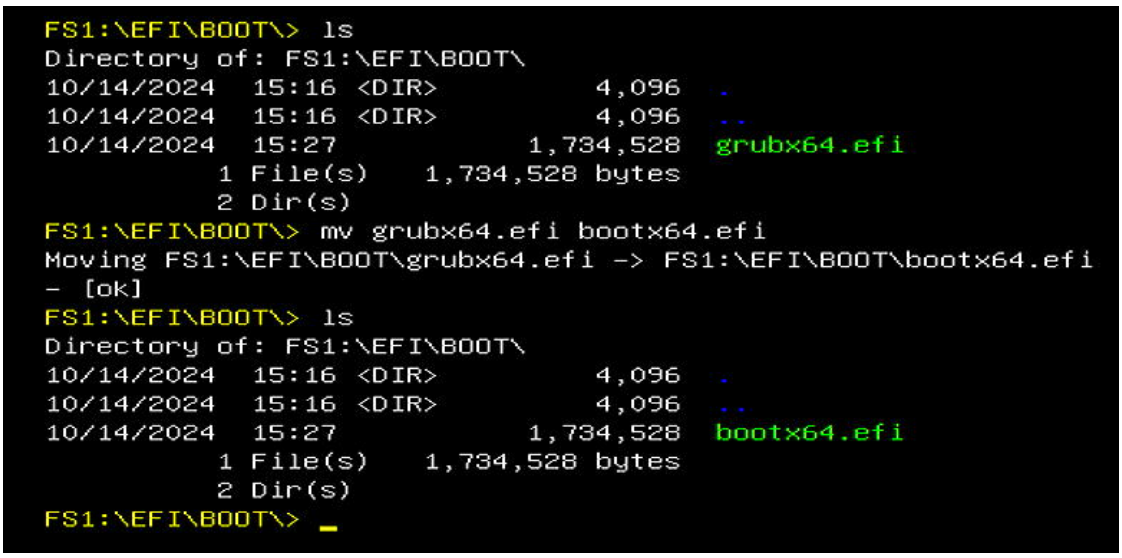

Рисунок 63 - Переименование загрузочного файла

10. Проверить продолжение загрузки в операционную систему.

11. Если загрузка в ОС не происходит, можно скопировать остальные файлы из подкаталога ubuntu в подкаталог BOOT (рисунок 64):

- *cd ubuntu*
- *cp * FS1:\EFI\BOOT*

Убедиться, что ОС загружается.

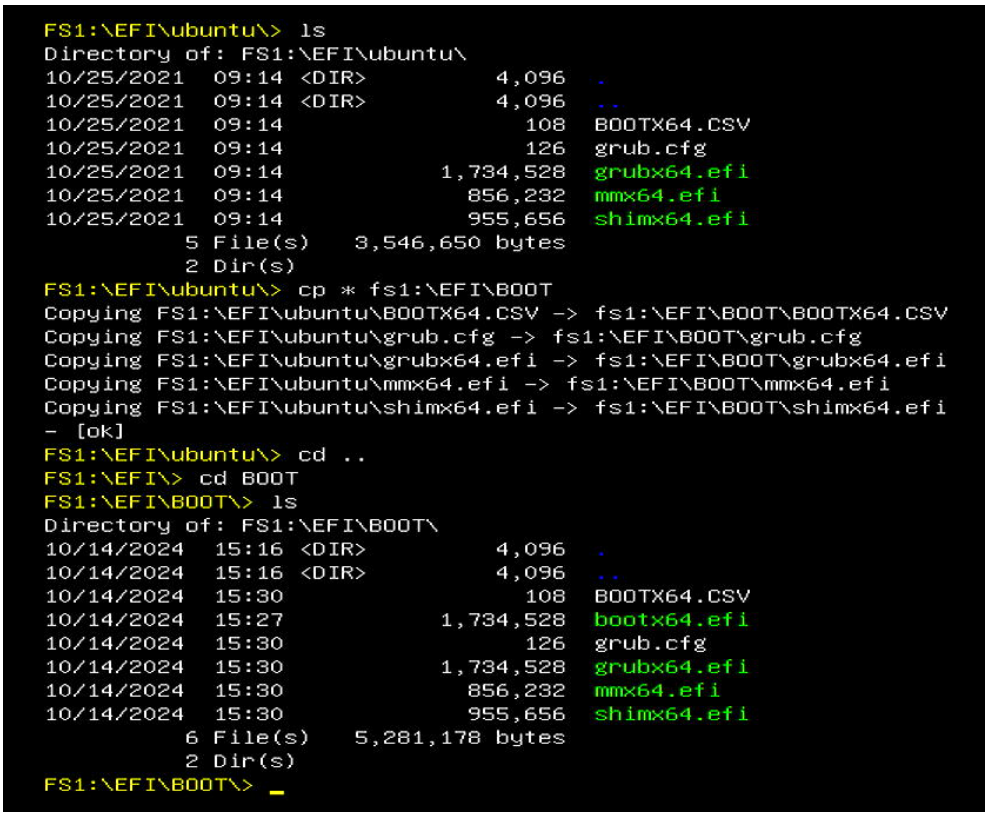

Рисунок 64 - Копирование дополнительных файлов в подкаталог BOOT