ОКБ
ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

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

Руководство пользователя

11443195.4012.046 34

Листов 22

Москва
2018

АННОТАЦИЯ

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

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

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

Применение защитных средств комплекса должно дополняться общими мерами технической безопасности.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

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

ПРИНЯТЫЕ ТЕРМИНЫ И ОБОЗНАЧЕНИЯ

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

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

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

Пользователь – субъект доступа к объектам (ресурсам) СВТ.

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

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

1. Общие сведения

1.1. Назначение комплекса

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

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

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

– несанкционированный доступ к информации за счет загрузки нештатной операционной системы и обхода правил разграничения доступа штатной операционной системы и (или) других средств защиты информации, работающих в среде штатной операционной системы;

– нарушение целостности программной среды средств вычислительной техники и (или) состава компонентов аппаратного обеспечения средств вычислительной техники в информационной системе;

– нарушение целостности программного обеспечения средства доверенной загрузки;

– несанкционированное изменение конфигурации (параметров) средств доверенной загрузки;

– преодоление или обход функций безопасности средств доверенной загрузки.

Комплекс начинает работу сразу после выполнения кода системного BIOS компьютера – до загрузки операционной системы, и позволяет обеспечить возможность доверенной загрузки[1] для ОС, поддерживающих файловые системы: FAT12, FAT16, FAT32, NTFS, HPFS, Ext2, Ext3, Ext4, ReiserFS, FreeBSD UFS/UFS2, Solaris UFS, QNX4, MINIX.

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

ПАК СЗИ НСД «ИНАФ» обеспечивает:

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

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

При модификации системного ПО замена контроллера не требуется.

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

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

которых отсутствуют PCI-слоты, но имеются свободные внутренние или внешние USB-разъемы.

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

1.2. Состав комплекса

Комплекс «ИНАФ» выпускается в программно-аппаратном исполнении.

Состав комплекса «ИНАФ»:

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

– функциональное программное обеспечение (далее по тексту – ФПО), которое является ядром защиты комплекса, реализует функциональные требования безопасности комплекса и исполняется в резидентной операционной среде, предустановленной на специализированный контроллер.

Резидентная операционная среда включает:

– резидентные драйверы специализированных контроллеров;

– резидентные драйверы персональных идентификаторов.

В состав ФПО комплекса входят следующие функциональные модули:

– средства идентификации пользователей;

– средства аутентификации пользователей;

– средства контроля целостности технических средств ПЭВМ (PC);

– средства контроля целостности системных областей жесткого диска;

– средства контроля целостности программных средств;

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

– средства аудита (работа с журналом регистрации событий);

– средства администрирования комплекса (среда администрирования).

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

Среда администрирования является частью комплекса «ИНАФ» и не требует установки какого-либо дополнительного ПО. С помощью нее администратор ПАК «ИНАФ» может добавлять и удалять пользователей, назначать пользователям идентификаторы и пароли, контролировать аппаратную часть ПЭВМ, прикладные и системные файлы, получать доступ к системному журналу контроллера.

1.3. Условия применения комплекса

1.3.1. Технические условия, необходимые для применения комплекса

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

- ПЭВМ типа IBM PC, сервер или рабочая станция, основанная на процессоре с архитектурой x86 (IA-32) или x86-64 (AMD64), с объемом динамической оперативной памяти (RAM) не менее 128 Мб, функционирующая под управлением операционной системы, поддерживающей любую из файловых систем, приведенных в подразделе 1.1 настоящего руководства;
- наличие свободного USB-разъема на корпусе СВТ или штырькового USB-разъема на материнской плате СВТ, соответствующего варианту исполнения специализированного контроллера «ИНАФ».

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

В составе ПЭВМ (PC), в котором установлен комплекс СЗИ НСД, должны отсутствовать средства, позволяющие за счет воздействия со стороны пользователей на штатные органы управления ПЭВМ (PC) воспрепятствовать передаче управления комплексу стандартной процедурой ROM Scan.

2. Установка и настройка комплекса

Установка и настройка комплекса СЗИ НСД «ИНАФ» осуществляется обладающим соответствующими полномочиями администратором комплекса и описана в и «Руководстве администратора» (11443195.4012.046 90).

3. Функции и интерфейсы пользователя

3.1. Функции пользователя

Процесс работы оператора (пользователя) на ПЭВМ, защищенной от несанкционированного доступа с использованием комплекса «ИНАФ», можно разделить на 3 этапа:

1) выполнение контрольных процедур при запуске ПЭВМ (применение доступных пользователям функций безопасности, которые предоставлены СДЗ):

- процедура идентификации оператора (пользователя);
- процедура аутентификации (подтверждение достоверности) оператора (пользователя);
- контроль целостности аппаратной части ПЭВМ, программ и данных, системных областей диска и системного реестра Windows;
- смена пароля, выполняемая, когда время жизни пароля превысило установленный администратором интервал времени;
- смена пароля в произвольный момент времени.

2) работа оператора (пользователя) в соответствии с функциональными обязанностями и правами доступа;

3) завершение работы.

3.2. Интерфейсы пользователя

Работа пользователя с комплексом «Аккорд-АМДЗ» выполняется с помощью графического интерфейса пользователя и описана в разделе 4 настоящего руководства.

4. Порядок работы на ПЭВМ с установленным комплексом

4.1. Выполнение контрольных процедур

Контрольные процедуры делятся на обязательные, которые по умолчанию выполняются при каждом запуске ПЭВМ, и необязательные, которые устанавливаются администратором комплекса.

К обязательным процедурам контроля относятся:

- процедура идентификации оператора (пользователя);
- процедура аутентификации (подтверждение достоверности) оператора (пользователя);
- контроль целостности аппаратной части ПЭВМ;
- проверка целостности системных областей диска и системного реестра;
- проверка целостности программ и данных;

К необязательным процедурам контроля относятся:

- процедура смены пароля, выполняемая, когда время жизни пароля превысило установленный администратором интервал времени;
- проверка ограничения на время входа оператора (пользователя) в систему.

4.1.1. Процедура идентификации оператора (пользователя)

При включении ПЭВМ, защищенной комплексом «ИНАФ», управление загрузкой передается контроллеру комплекса, при этом на экран выводится окно входа в систему с запросом идентификатора (рисунок 1).

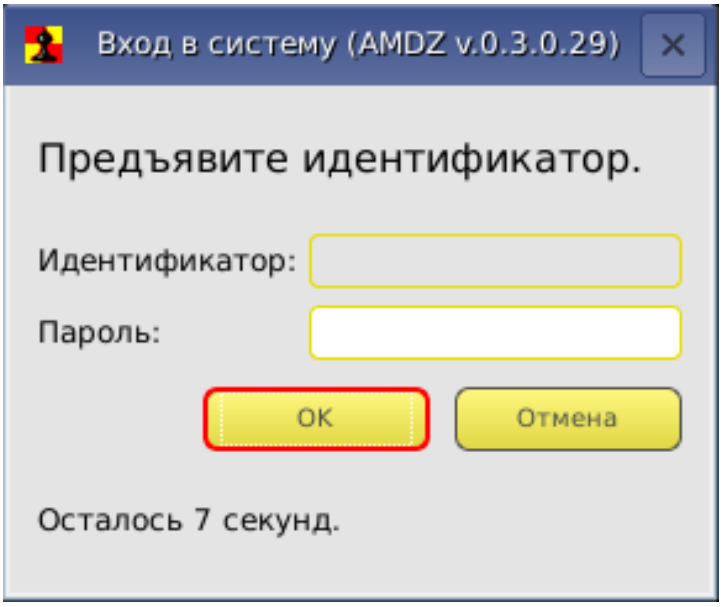

Рисунок 1 – Окно входа в систему с запросом идентификатора

Окно остается на мониторе до момента предъявления идентификатора пользователя или до момента истечения интервала времени, отведенного для процедуры начальной идентификации.

В случае если в память идентификатора не записан секретный ключ пользователя или если идентификатор некорректно предъявлен, на экран выводится сообщение об ошибке, сопровождаемое звуковым сигналом (рисунок 2) и пользователю предлагается повторить процедуру идентификации.

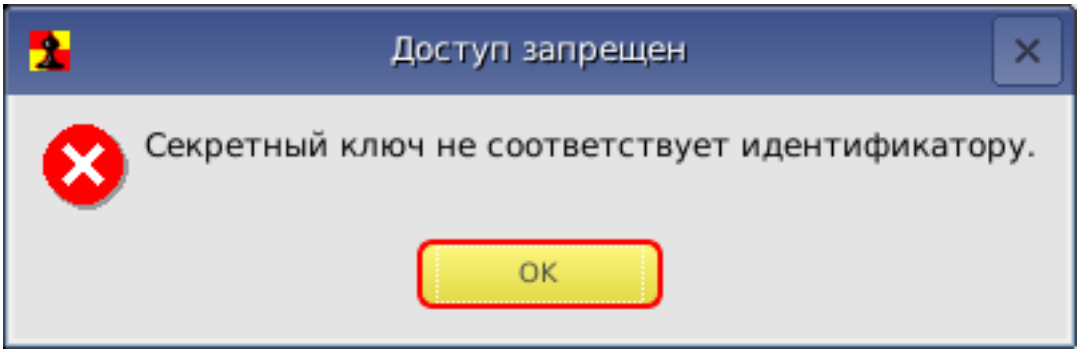

Рисунок 2 – Сообщение об ошибке

В случае предъявления идентификатора, незарегистрированного в базе текущего контроллера «Аккорд-АМДЗ», на экран выводится сообщение «Незарегистрированный пользователь!».

При успешном завершении описанной процедуры идентификации оператора (пользователя) в поле «Идентификатор» окна входа в систему появляется номер соответствующего идентификатора. Далее следует перейти к выполнению процедуры аутентификации (подтверждения достоверности) (см. 4.1.2).

4.1.2. Процедура аутентификации (подтверждение достоверности)

После идентификации оператора (пользователя), при условии, что ему при регистрации был задан пароль для входа в систему, в окне входа в систему появляется запрос на введение пароля (рисунок 3).

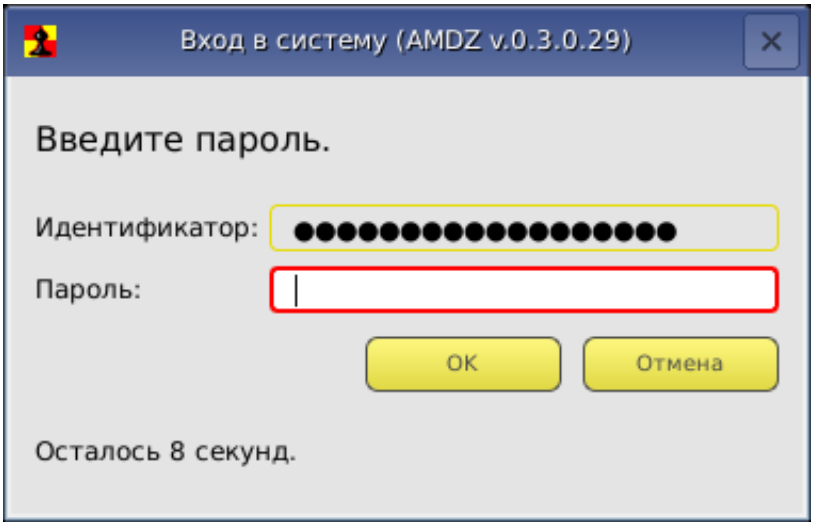

Рисунок 3 – Окно входа в систему с запросом на введение пароля

Необходимо набрать свой личный пароль (при этом символы пароля отображаются на экране в виде звездочек (*)) и нажать клавишу <Enter>.

После успешного завершения описанной процедуры контроллер переходит к следующему этапу – проверке целостности аппаратной части ПЭВМ (см. 4.1.3).

При неправильно введенном пароле на экран выводится соответствующее сообщение (рисунок 4) и оператору (пользователю) предлагается снова пройти процедуры идентификации и аутентификации (подтверждения достоверности).

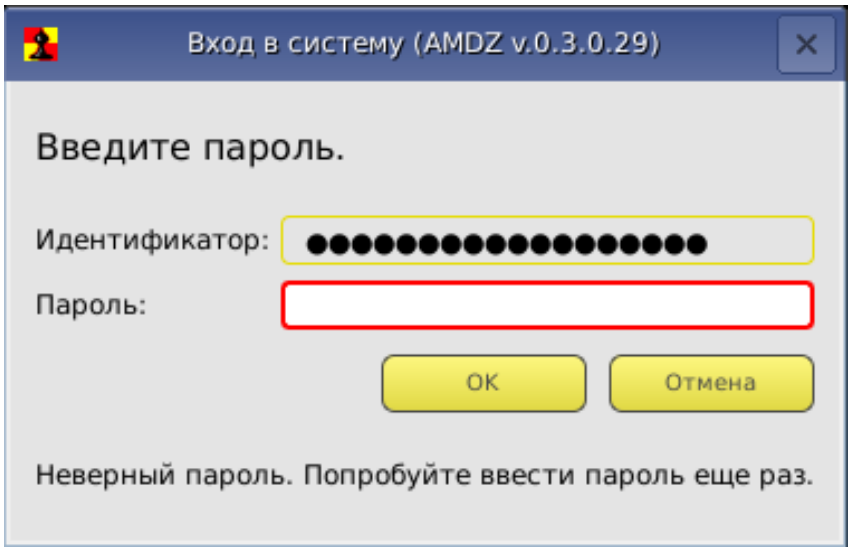

Рисунок 4 – Сообщение о неверно введенном пароле

При превышении установленного администратором числа неверных попыток ввода пароля ПЭВМ блокируется. Продолжить работу можно только после перезагрузки ПЭВМ (рисунок 5).

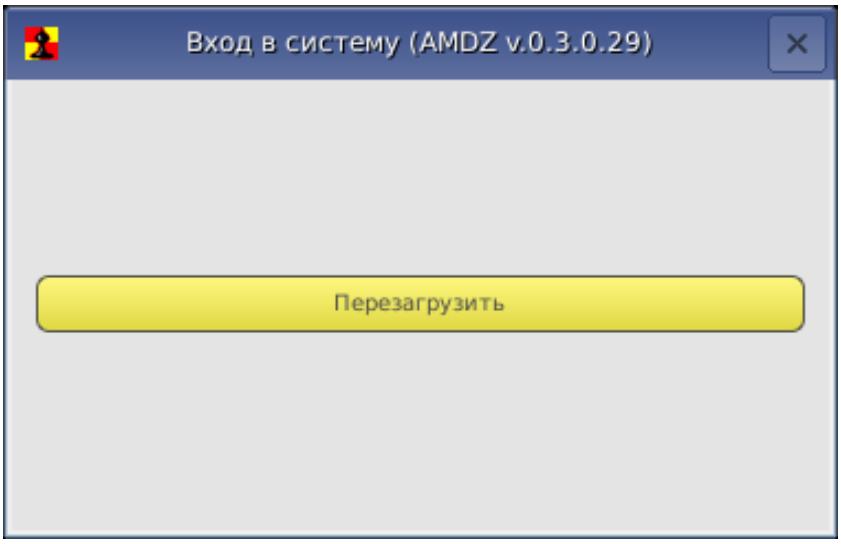

Рисунок 5 – Исчерпан лимит попыток идентификации

В случае если пользователю не назначен пароль, процедура аутентификации не выполняется и контроллер сразу переходит к проверке целостности аппаратной части ПЭВМ (при условии успешного выполнения идентификации).

Если в процессе идентификации предъявлен идентификатор оператора (пользователя), который уже инициализирован в СЗИ «ИНАФ», но на данной ПЭВМ этот идентификатор не зарегистрирован, все равно происходит запрос пароля пользователя. После ввода пароля выводится сообщение «Незарегистрированный пользователь!», а номер идентификатора заносится в системный журнал с пометкой «Неизвестный идентификатор».

4.1.3. Процедура контроля целостности аппаратной части ПЭВМ

На этом этапе проводится проверка состава устройств, установленных на данной ПЭВМ. В случае если нарушен состав аппаратной части ПЭВМ, выводится окно, вариант которого показан на рисунке 6 (при загрузке под учетной записью пользователя в данном окне доступна только кнопка <Перезагрузить>). При этом загрузка ОС не производится. Загрузка будет возможна только после вмешательства администратора.

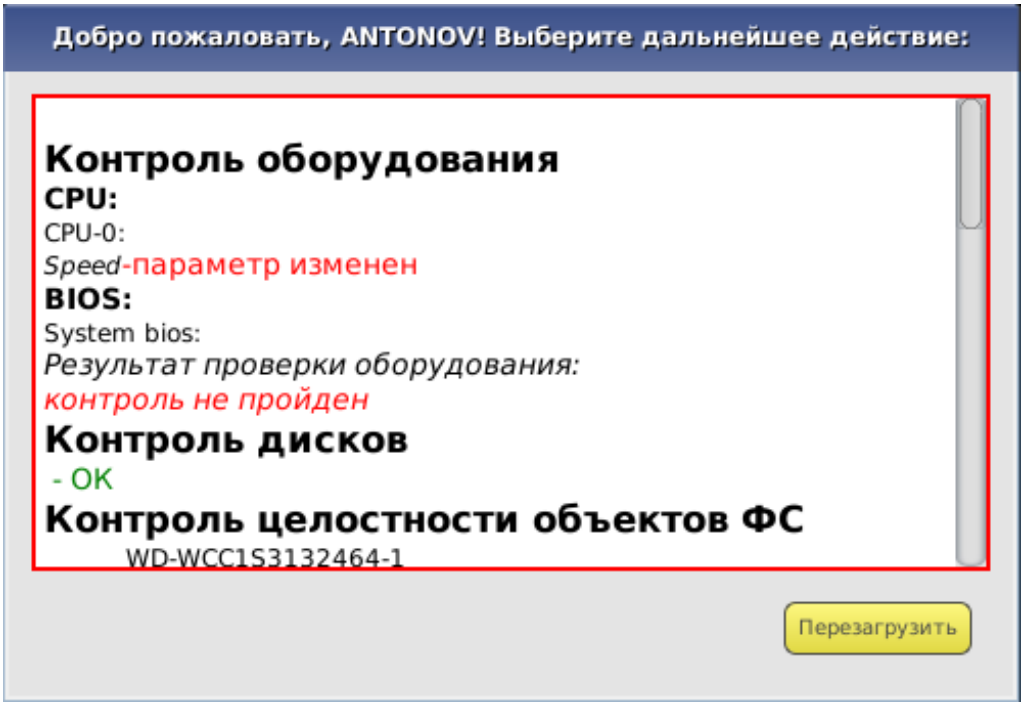

Рисунок 6 – Окно контроля целостности аппаратной части ПЭВМ

4.1.4. Процедура контроля целостности системных областей, системных файлов, программ и данных

Данная процедура предназначена для исключения несанкционированных модификаций (случайных или злоумышленных) программной среды, обрабатываемой информации, системных областей и системных файлов. Осуществляется до загрузки ОС.

При проверке целостности вычисляется контрольная сумма файлов, которая сравнивается с эталонным значением, хранящимся в контроллере. Эти данные заносятся администратором в процессе настройки контроля целостности и могут меняться в процессе эксплуатации ПЭВМ.

Если в ходе выполнения процедуры контроля целостности программной среды, обрабатываемой информации, системных областей и системных файлов

нарушена целостность защищаемых файлов, выводится соответствующее сообщение и загрузка ОС не производится. Загрузка будет возможна только после вмешательства администратора комплекса (входа в систему с помощью его персонального идентификатора).

4.1.5. Смена пароля по истечении срок его действия

В случае когда время «жизни» пароля превысило отведенный интервал времени действия данного пароля, необходимо выполнить процедуру смены пароля.

Временной интервал действия пароля оператора (пользователя) устанавливается администратором при регистрации пользователя, либо при последующем администрировании системы. По решению администратора оператору (пользователю) может предоставляться право самостоятельной смены пароля.

Если пользователь не имеет права на смену пароля, то при вводе пароля с истекшим сроком действия на экран выводится сообщение, показанное на рисунке 7. В таком случае для смены пароля необходимо обратиться к администратору.

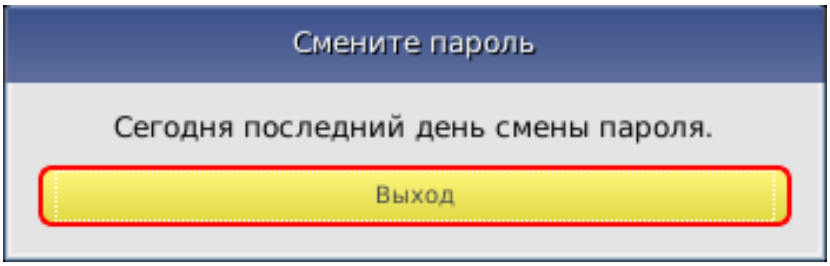

Рисунок 7 – Сообщение о необходимости смены пароля в случае если пользователь (оператор) не обладает соответствующими правами

Если оператору (пользователю) предоставлено право самостоятельной смены пароля, при вводе пароля с истекшим сроком действия на экран выводится окно, показанное на рисунке 8.

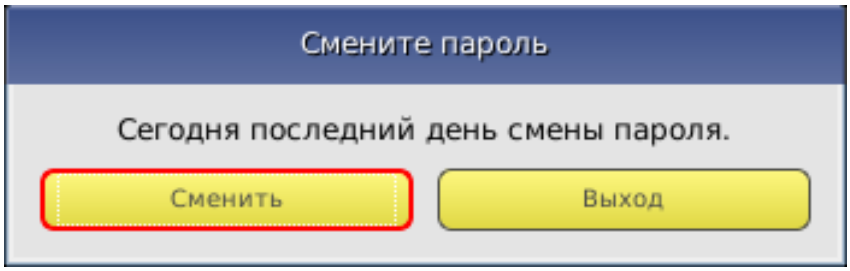

Рисунок 8 – Сообщение о необходимости смены пароля в случае если пользователь (оператор) обладает соответствующими правами

Для выполнения процедуры смены пароля следует нажать кнопку <Сменить>. На экран выводится окно смены пароля, показанное на рисунке 9.

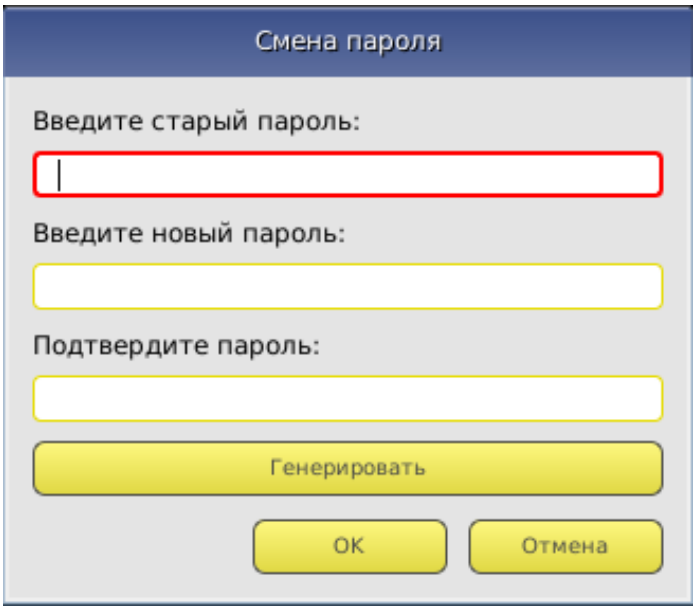

Рисунок 9 – Окно смены пароля

В данном окне необходимо ввести старый пароль, указать новый[1] пароль, а также подтвердить новый пароль его повторным вводом в соответствующее поле и нажать клавишу <OK>. Также имеется возможность генерировать новый пароль автоматически, нажав кнопку <Генерировать>.

ВНИМАНИЕ! Если длина вводимого пароля меньше заданного администратором количества символов, то выводится сообщение об ошибке.

ВНИМАНИЕ! Не допускается ввод в качестве пароля последовательностей типа: '123456…' или 'qwerty…'. При вводе подобных последовательностей символов выдается сообщение об ошибке.

Если новый пароль подтвержден правильно, то выводится сообщение о том, что новый пароль успешно установлен, и продолжается работа контроллера.

При нажатии клавиши <Отмена> смена пароля не выполняется, продолжается работа контроллера, при этом число попыток для смены пароля уменьшается на единицу. Если число попыток исчерпано, то выводится сообщение, показанное на рисунке 10.

[1] Пароль может состоять из букв, цифр и специальных символов. Символы могут вводиться как в верхнем, так и в нижнем регистре. Вводимые символы на экране отображаются звездочками (*). При несовпадении введенных последовательностей выводится сообщение об ошибке. В этом случае операцию придется повторить.

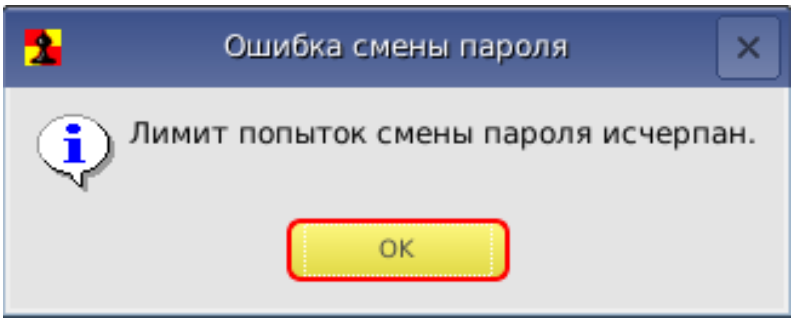

Рисунок 10 – Сообщение об исчерпании лимита попыток смены пароля

ВНИМАНИЕ! Оператор (пользователь) может сменить пароль на новый во время любой из попыток, но при этом должен помнить - когда число попыток станет равным нулю, загрузка системы произойдет только после вмешательства администратора комплекса.

Если оператору (пользователю) предоставлено право самостоятельной смены пароля, он может сменить действующий пароль на новый в соответствии с правилами смены паролей. Эти правила должны быть оговорены в отдельной инструкции. Процедура смены пароля выполняется в соответствии с сообщениями, выводимыми на экран монитора, в порядке, указанном выше.

4.1.6. Смена пароля в произвольный момент времени (по инициативе пользователя)

В случае если по каким-либо причинам у пользователя возникла необходимость сменить пароль до истечения срока его действия (и если это действие не запрещено для данного пользователя администратором), имеется возможность выполнить процедуру смены пароля в произвольный момент времени.

В случае если пользователю ранее не был назначен пароль, после прохождения процедуры идентификации пользователь может назначить его, зажав кнопку <Ctrl> и предъявив идентификатор, а затем выполнив процедуру смены пароля, описанную в п. 4.1.5 настоящего руководства.

В случае если пользователю ранее уже был назначен пароль, после прохождения процедур идентификации и аутентификации он может сменить его любым из следующих способов:

1) предъявить идентификатор, ввести действующий пароль и нажать клавиши <Ctrl>+<Enter>. В появившемся далее окне смены пароля (рисунок 9) выполнить процедуру смены пароля, описанную в п. 4.1.5 настоящего руководства;

2) предъявить идентификатор, нажать клавиши <Ctrl>+<Enter> (при этом появится сообщение «Неверный пароль»), ввести действующий пароль и нажать клавишу <Enter>. В появившемся далее окне смены пароля (рисунок 9) выполнить процедуру смены пароля, описанную в п. 4.1.5 настоящего руководства.

4.1.7. Проверка ограничения на время входа оператора (пользователя) в систему

Если администратор комплекса установил для оператора (пользователя) ПЭВМ ограничение по времени входа в систему, проверка этого параметра проводится после всех остальных контрольных процедур.

Если оператору (пользователю) ПЭВМ запрещен вход в систему в данное время, на экран выводится сообщение, показанное на рисунке 11.

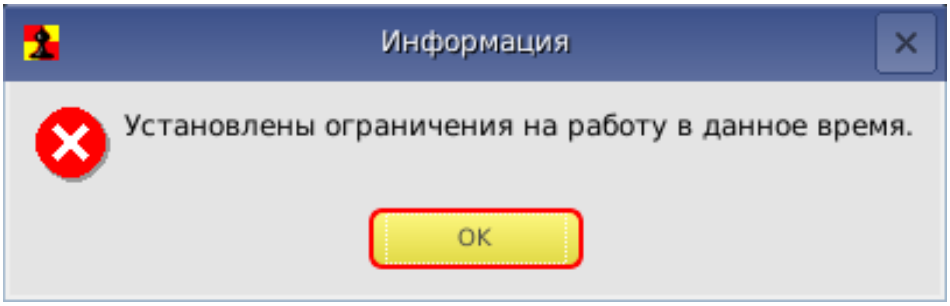

Рисунок 11 – Сообщение о наличии ограничений на работу в данное время

При этом загрузка операционной системы не выполняется. Порядок действий оператора (пользователя) в данной ситуации указан в таблице 1 (см. раздел 4 настоящего Руководства).

4.2. Работа оператора (пользователя) в соответствии с функциональными обязанностями

После положительного результата выполнения контрольных процедур осуществляется загрузка операционной системы и оператор (пользователь) может приступить к работе, в соответствии с его функциональными обязанностями и правами доступа.

Порядок работы оператора (пользователя) на ПЭВМ в соответствии с его функциональными обязанностями и правами доступа регламентируется отдельными инструкциями.

4.3. Завершение работы

Завершение работы прикладных программ происходит в порядке, установленном для конкретного прикладного программного обеспечения и описанном в соответствующих руководствах.

5. Обязанности пользователя, необходимые для безопасной эксплуатации СДЗ

Для безопасной эксплуатации комплекса «Аккорд-АМДЗ» пользователь обязан выполнять все обязательные процедуры контроля, указанные в п. 4.1 настоящего руководства.

ВНИМАНИЕ! Всем пользователям комплекса «ИНАФ» запрещается передавать третьим лицам сведения о паролях от своих учетных записей, а также зарегистрированные для них персональные идентификаторы.

6. Техническая поддержка

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

+7 (495) 994-49-96

+7 (495) 994-49-97

+7 (926) 235-89-17

+7 (926) 762-17-72

или по адресу электронной почты help@okbsapr.ru

Наш адрес в Интернете http://www.okbsapr.ru/

Приложение 1.
Наименование и результат операций в системном журнале

Сообщение на экране	Причины появления сообщения	Порядок действий
«Секретный ключ не соответствует идентификатору»	Идентификатор был некорректно предъявлен	Повторно выполнить процедуру предъявления идентификатора (после появления на экране соответствующего запроса)
«Установлены ограничения на работу в данное время»	В соответствии с установленными правилами доступа для данного оператора (пользователя) не разрешен вход в систему в данное время	1. Вызвать администратора. 2. Уточнить разрешенное время работы с учетом принятых ПРД. 3. Администратор (при необходимости) должен установить разрешенный интервал времени для работы данного оператора (пользователя)
«Сегодня последний день смены пароля»	Окончилось время «жизни» установленного пароля	1. Вызвать администратора (если не предоставлено право самостоятельной смены пароля). 2. Изменить (установить) необходимые параметры пароля в соответствии с принятыми правилами. 3. Самостоятельно установить необходимые параметры пароля в соответствии с принятыми правилами, если на это предоставлено право
«Лимит попыток смены пароля исчерпан»	Закончились все предоставленные попытки смены пароля	1. Вызвать администратора. 2. Сменить пароль с помощью администратора
«Незарегистрированный пользователь!»	Предъявлен незарегистрированный идентификатор	Предъявить зарегистрированный идентификатор и повторить процедуру идентификации
«Неверный пароль. Попробуйте ввести пароль еще раз»	Неправильно введен пароль	Ввести правильный пароль