ОКБ ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

Модуль доверенной загрузки «Аккорд-МКТ»

Руководство пользователя (оператора)

37222406.501410.071 34
37222406.26.20.40.140.082 34

Листов 19

Москва
2020

АННОТАЦИЯ

Настоящий документ является руководством пользователя на изделие «Модуль доверенной загрузки «Аккорд-МКТ» (далее по тексту – изделие «Аккорд-МКТ», изделие, «Аккорд-МКТ», МДЗ «Аккорд-МКТ») и содержит описание способов использования средств защиты изделия, его интерфейса с пользователем в процессе обработки информации.

В документе приведены основные функции и особенности эксплуатации МДЗ «Аккорд-МКТ» с точки зрения пользователя.

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

Пояснения – замечания в описании некоторых команд, содержащие рекомендации администратору БИ по порядку использования этих команд. Пояснения выделены мелким шрифтом.

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

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ	- автоматизированное рабочее место
АС	- автоматизированная система
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

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) ЭВМ на базе процессоров с архитектурой x86_64 (ТУ 501410-071-37222406-2016, ТУ 26.20.40.140-082-37222406-2019) 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 12 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 12 буквенно-цифровых символов, введенных с клавиатуры;
- контроль целостности отдельных файлов 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 базовую систему ввода-вывода (БСВВ) ЭВМ на базе процессоров с архитектурой x86_64 (ТУ 501410-071-37222406-2016, ТУ 26.20.40.140-082-37222406-2019) 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 БСВВ выполняется производителем изделия на этапе изготовления ЭВМ.

1.3. Условия применения МДЗ «Аккорд-МКТ»

СПО «Аккорд-МКТ» встраивается производителем в БСВВ ЭВМ на этапе изготовления и функционирует в ее составе.

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.

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

2. Настройка МДЗ «Аккорд-МКТ»

Настройка МДЗ «Аккорд-МКТ» осуществляется обладающим соответствующими полномочиями администратором и описана «Руководстве администратора» (37222406.501410.071 90 37222406.26.20.40.140.082 90).

3. Функции и интерфейсы пользователя

3.1. Функции пользователя

Процесс работы оператора (пользователя) на ЭВМ, защищенной от несанкционированного доступа с использованием МДЗ «Аккорд-МКТ», можно разделить на 3 этапа:

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

- процедура идентификации оператора (пользователя);
- процедура аутентификации (подтверждение достоверности) оператора (пользователя);
- процедура контроля целостности (файлов, загрузочных метаданных);
- смена пароля, выполняемая, когда время жизни пароля превысило установленный администратором интервал времени;
- смена пароля в произвольный момент времени (по инициативе пользователя);

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

3) завершение работы.

3.2. Интерфейсы пользователя

Работа пользователя с МДЗ «Аккорд-МКТ» выполняется с помощью графического интерфейса пользователя и описана в разделе 4 настоящего Руководства.

4. Порядок работы на ЭВМ с установленным МДЗ «Аккорд-МКТ»

Процесс работы оператора (пользователя) на ЭВМ, защищенной от несанкционированного доступа с использованием МДЗ «Аккорд-МКТ», можно разделить на 3 этапа:

1. Выполнение контрольных процедур при запуске ЭВМ.
2. Работа оператора (пользователя) в соответствии с функциональными обязанностями и правами доступа.
3. Завершение работы и выход из системы.

4.1. Выполнение контрольных процедур

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

К обязательным процедурам контроля относятся:

- процедура самотестирования МДЗ «Аккорд-МКТ»;
- процедура идентификации оператора (пользователя);
- процедура аутентификации (подтверждение достоверности) оператора (пользователя);
- проверка целостности отдельных файлов и программных средств ЭВМ.

К необязательным процедурам контроля относятся:

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

4.1.1. Процедура самотестирования МДЗ «Аккорд-МКТ»

При включении ЭВМ, защищенной МДЗ «Аккорд-МКТ», управление загрузкой передается МДЗ «Аккорд-МКТ», который инициирует самотестирование модулей «Аккорд-МКТ». В случае нарушения целостности на данном этапе появляется соответствующее сообщение (рисунок 1), после чего начинается перезагрузка компьютера.

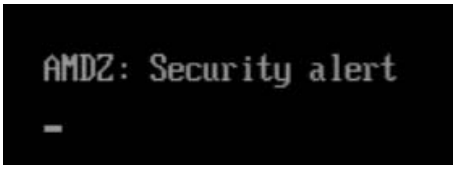

Рисунок 1 – Сообщение о нарушении целостности при самотестировании МДЗ «Аккорд-МКТ»

О нарушении целостности пользователь обязан сообщить администратору БИ.

4.1.2. Процедура идентификации оператора (пользователя)

При успешном прохождении этапа самотестирования на экран выводится окно входа в систему с запросом идентификатора (рисунок 2).

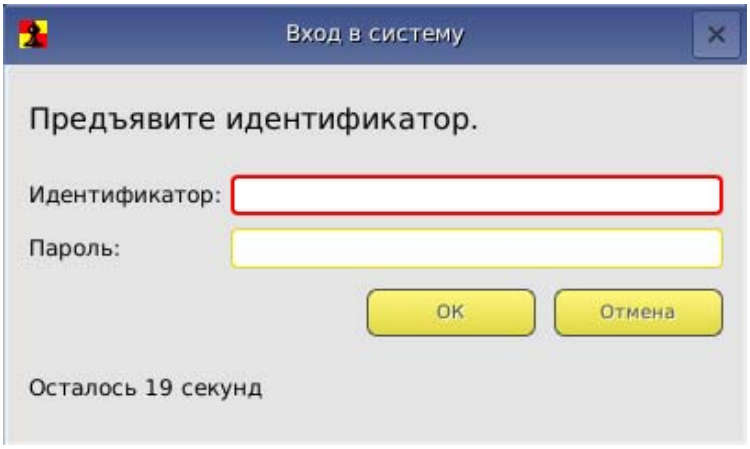

Рисунок 2 – Окно входа в систему с запросом идентификатора

В стандартном режиме загрузки ОС при появлении этого окна следует предъявить идентификатор (ТУ 501410-071-37222406-2016, ТУ 26.20.40.140-082-37222406-2019) или ввести его в соответствующее поле (ТУ 501410-071-37222406-2016) и затем перейти к выполнению процедуры аутентификации (подтверждения достоверности) (см. 4.1.3).

В режиме загрузки ОС, предполагающем только контроль целостности, следует выдержать установленный таймаут, после чего МДЗ «Аккорд-МКТ» переходит к проверке целостности. Если этот режим расширен вводом дополнительных данных, то пользователю следует выдержать установленный таймаут, а после успешного прохождения МДЗ «Аккорд-МКТ» процедуры контроля целостности ввести свои идентификационные данные в появившееся окно (рисунок 3). При вводе логина доменного пользователя должен использоваться следующий формат: «domain.com\username».

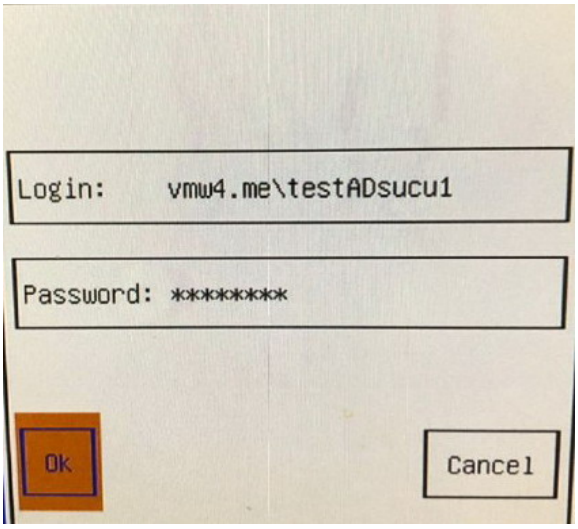

Рисунок 3 – Окно ввода дополнительных данных

4.1.3. 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.

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

После успешного завершения описанной процедуры МДЗ «Аккорд-МКТ» переходит к следующему этапу – проверке целостности объектов по спискам контроля (см. 4.1.4).

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

При троекратном неправильном вводе пароля загрузка блокируется. Продолжить работу можно только после выполнения перезагрузки.

В случае если пользователю не назначен пароль, процедура аутентификации не выполняется, и МДЗ «Аккорд-МКТ» сразу переходит к проверке целостности (при условии успешного выполнения идентификации).

4.1.4. Процедура контроля целостности

Данная процедура предназначена для исключения несанкционированных модификаций (случайных или злоумышленных) программной среды и обрабатываемой информации, если они поставлены на контроль целостности. Осуществляется до загрузки ОС.

При проверке целостности вычисляется контрольная сумма файлов, которая сравнивается с эталонным значением, хранящимся в МДЗ «Аккорд-МКТ». Эти данные заносятся администратором в процессе настройки контроля целостности и могут меняться в процессе эксплуатации МДЗ «Аккорд-МКТ».

Если в ходе выполнения процедуры контроля целостности программной среды и обрабатываемой информации нарушена целостность защищаемых файлов, выводится соответствующее сообщение (рисунок 4), и загрузка ОС не производится. Загрузка будет возможна только после вмешательства администратора БИ (входа в систему с помощью его идентификатора).

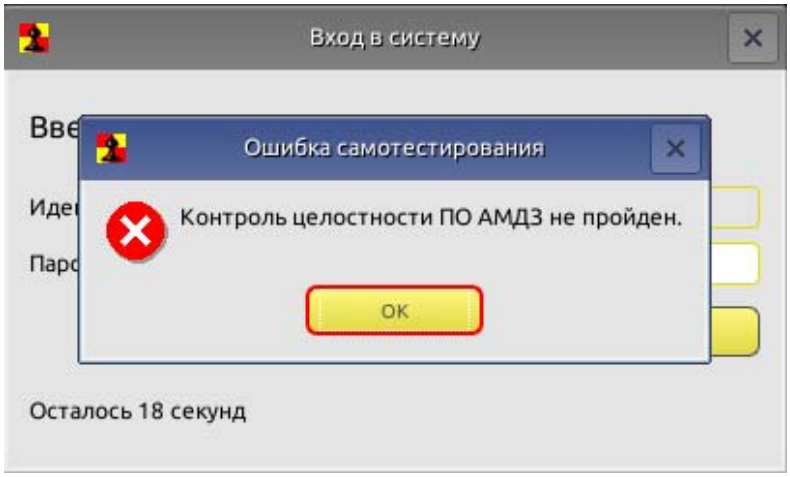

Рисунок 4 – Сообщение о нарушении целостности ПО

При успешном завершении процедуры контроля целостности ПО пользователю будет предложено продолжить загрузку ОС (рисунок 5).

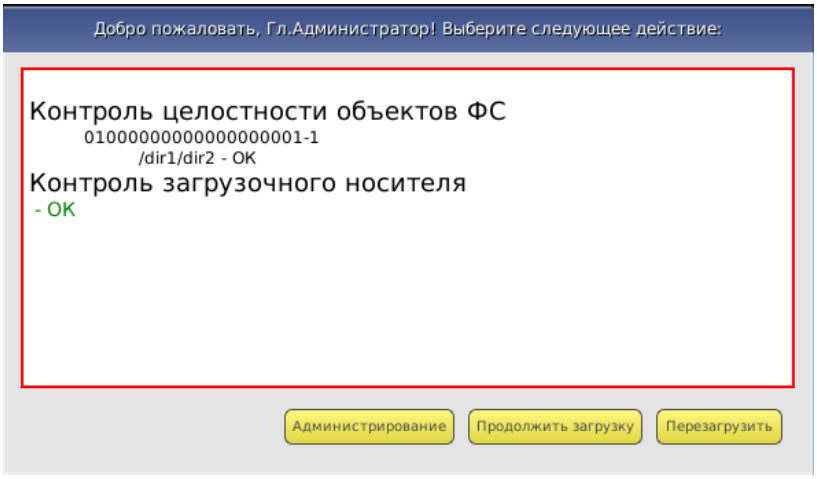

Рисунок 5 – Окно контроля целостности в случае успешного прохождения контроля

4.1.5. Смена пароля по истечении срока 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 БИ при регистрации пользователя либо при последующем администрировании системы. По решению администратора БИ 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 6. В таком случае для смены пароля необходимо обратиться к администратору БИ.

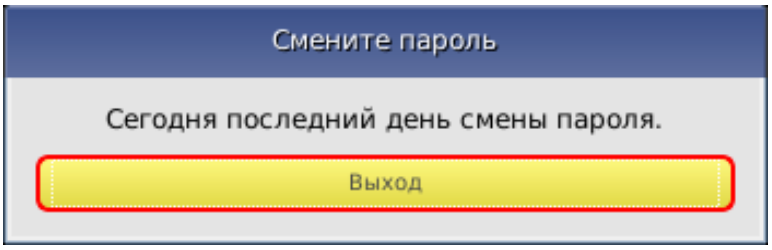

Рисунок 6 – Сообщение о необходимости смены пароля в случае если пользователь (оператор) не обладает соответствующими правами

Если оператору (пользователю) предоставлено право самостоятельной смены пароля, при вводе пароля с истекшим сроком действия на экран выводится окно, показанное на рисунке 7.

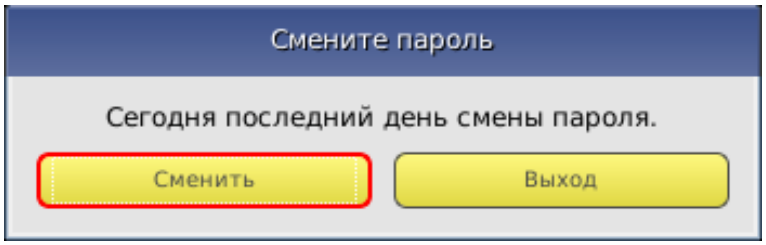

Рисунок 7 – Сообщение о необходимости смены пароля, в случае если пользователь (оператор) обладает соответствующими правами

Для выполнения процедуры смены пароля следует нажать кнопку <Сменить>. На экран выводится окно смены пароля, показанное на рисунке 8.

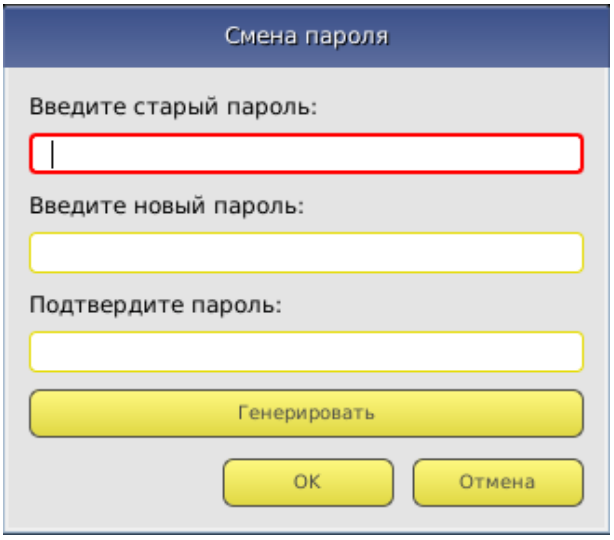

Рисунок 8 – Окно смены пароля

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, 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.

[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.

Если новый пароль подтвержден правильно, выводится сообщение о том, что новый пароль успешно установлен, и работа МДЗ «Аккорд-МКТ» продолжается.

При нажатии клавиши <Отмена> смена пароля не выполняется, продолжается работа МДЗ «Аккорд-МКТ», при этом число попыток для смены пароля уменьшается на единицу. Если число попыток исчерпано, выводится сообщение, показанное на рисунке 9.

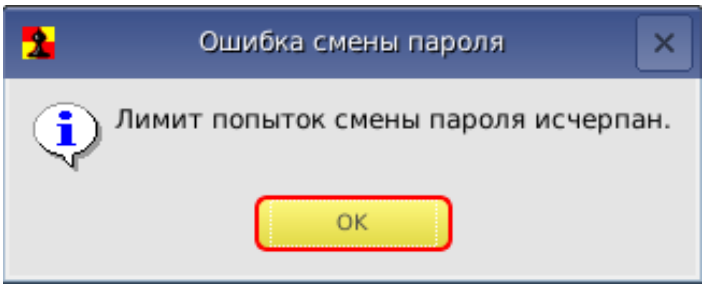

Рисунок 9 – Сообщение об исчерпании лимита попыток смены пароля

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 БИ.

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 БИ), 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)предъявив идентификатор, ввести действующий пароль и нажать клавиши <Ctrl>+<Enter>. В появившемся далее окне смены пароля (рисунок 8) выполнить процедуру смены пароля, описанную в п. 4.1.5 настоящего Руководства;

2)предъявив 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 8) выполнить процедуру смены пароля, описанную в п. 4.1.5 настоящего Руководства.

4.1.7. Проверка ограничения времени входа оператора (пользователя) в систему

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

Если оператору (пользователю) запрещен вход в систему в данное время, на экран выводится сообщение, показанное на рисунке 10.

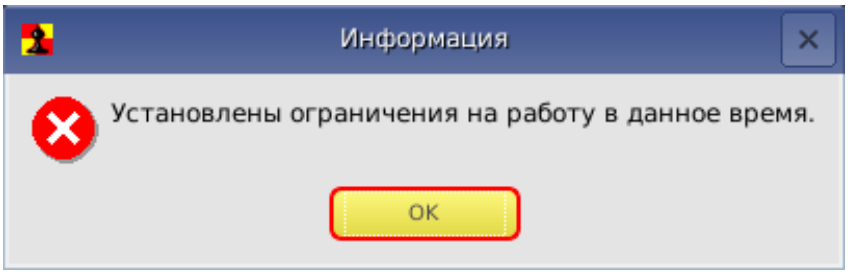

Рисунок 10 – Сообщение о наличии ограничений на работу в данное время

При этом загрузка операционной системы не выполняется.

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) в соответствии с его функциональными обязанностями и правами доступа регламентируется отдельными инструкциями.

4.3. Завершение работы и выход из системы

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 МДЗ «Аккорд-МКТ»

Для безопасной эксплуатации МДЗ «Аккорд-МКТ» пользователь обязан выполнять все обязательные процедуры контроля, указанные в разделе 4 настоящего Руководства.

ВНИМАНИЕ! Всем пользователям МДЗ «Аккорд-МКТ» запрещается передавать третьим лицам сведения о паролях от своих учетных записей, а также зарегистрированные для них 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
«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