ОКБ ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

Средство защиты информации от несанкционированного доступа для ПЭВМ (РС) «Аккорд-АМДЗ»

(Аппаратный модуль доверенной загрузки)

Руководство пользователя

11443195.4012.038 34
11443195.4012.054 34
37222406.26.20.40.140.079 34
37222406.26.20.40.140.097 34
37222406.26.20.40.140.102 34
37222406.26.20.40.140.108 34
РДСУ.26.20.40.140.113 34
37222406.26.20.40.140.115 34

Листов 26

Москва
2023

АННОТАЦИЯ

Настоящий документ является руководством пользователя средства защиты информации от НСД – аппаратного модуля доверенной загрузки – «Аккорд-АМДЗ», далее по тексту «Аккорд-АМДЗ», и предназначен для лиц, планирующих и организующих защиту информации с их использованием в системах и средствах информатизации на базе ПЭВМ.

В документе приведены основные функции и особенности эксплуатации комплексов СЗИ НСД «Аккорд-АМДЗ», работающих на основе контроллеров:

– Аккорд-5.5(e), Аккорд-LE, Аккорд-GX, Аккорд-GXM, Аккорд-GXMH (для СЗИ НСД «Аккорд-АМДЗ», выпускаемого по ТУ 4012-038-11443195-2011);

– Аккорд-GX, Аккорд-GXMH, Аккорд-GXM2 (для СЗИ НСД «Аккорд-АМДЗ», выпускаемого по ТУ 4012-054-11443195-2013 и ТУ 26.20.40.140-097-37222406-2021);

– Аккорд-GXM2 v.P, Аккорд-GXM2 v.S на базе микроконтроллера PIC18, Аккорд-GXM2 v.S на базе микроконтроллера PIC32 (для СЗИ НСД «Аккорд-АМДЗ», выпускаемых по ТУ 26.20.40.140-108-37222406-2022 и ТУ 26.20.40.140-115-37222406-2023);

– Аккорд-GX, Аккорд-GXM, Аккорд-GXMH, Аккорд-GXM2, Аккорд-GXM2 v.P, Аккорд-GXM2 v.S (для СЗИ НСД «Аккорд-АМДЗ», выпускаемого по ТУ 26.20.40.140-079-37222406-2019);

– Аккорд-GXM2 v.P, Аккорд-GXM2 v.S (для СЗИ НСД «Аккорд-АМДЗ», выпускаемого по ТУ 26.20.40.140-113-РДСУ-2023).

Перед установкой и эксплуатацией комплекса СЗИ НСД «Аккорд-АМДЗ» 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

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 комплексом «Аккорд», в том числе, учет выданных идентификаторов, осуществляет периодическое тестирование средств защиты комплекса.

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

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

Пользователь – субъект доступа к объектам (ресурсам) СВТ.

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

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

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АМДЗ	Аппаратный модуль доверенной загрузки
АБИ	Администратор безопасности информации
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ОС	Операционная система
ПК	Персональный компьютер
ПО	Программное обеспечение
ПРД	Правила (политики) разграничения доступа
ПЭВМ	Персональная электронно-вычислительная машина
РС	Рабочая станция
СВТ	Средство вычислительной техники
СЗИ	Средство защиты информации
ТУ	Технические условия

1. Общие сведения

1.1. Назначение комплекса

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

- в ФСТЭК России в соответствии с требованиями документов «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013), «Профиль защиты средства доверенной загрузки уровня платы расширения четвертого класса защиты. ИТ.СДЗ. ПР4.ПЗ» (ФСТЭК России, 2013) при выполнении ограничений, указанных в ТУ 4012-038-11443195-2011;
- в ФСБ России на соответствие требованиям к аппаратно-программным модулям доверенной загрузки ЭВМ по I классу защиты и классу сервиса Б (ТУ 4012-054-11443195-2013);
- в ФСБ России на соответствие требованиям к аппаратно-программным модулям доверенной загрузки ЭВМ по II классу защиты и классу сервиса Б (ТУ 26.20.40.140-108-37222406-2022 и ТУ 26.20.40.140-115-37222406-2023);
- в ФСБ России на соответствие требованиям к аппаратно-программным модулям доверенной загрузки ЭВМ по II классу защиты и классу сервиса А (ТУ 26.20.40.140-102-37222406-2021);
- в ФСБ России на соответствие требованиям к аппаратно-программным модулям доверенной загрузки ЭВМ по III классу защиты и классу сервиса Б (ТУ 26.20.40.140-097-37222406-2021);
- в ФСТЭК России в соответствии с требованиями документов «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013), «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2018) и «Профиль защиты средства доверенной загрузки уровня платы расширения второго класса защиты. ИТ.СДЗ.ПР2.ПЗ» (ФСЭК России, 2013) при выполнении ограничений, указанных в ТУ 26.20.40.140-079-37222406-2019 и ТУ 26.20.40.140-113-РДСУ-2023.

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

– несанкционированный доступ к информации за счет загрузки нештатной операционной системы (ОС) и обхода правил разграничения доступа

штатной ОС и (или) других средств защиты информации, работающих в среде штатной ОС;

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

– нарушение целостности программного обеспечения средства доверенной загрузки;

– несанкционированное изменение конфигурации (параметров) средств доверенной загрузки;

– преодоление или обход функций безопасности средств доверенной загрузки.

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

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

- FAT12, FAT16, FAT32, NTFS, HPFS, Ext2, Ext3, FreeBSD UFS/UFS2, Solaris UFS, QNX4, MINIX, Ext4, ReiserFS (ТУ 4012-054-11443195-2013, ТУ 26.20.40.140-097-37222406-2021);

- FAT12, FAT16, FAT32, NTFS, HPFS, Ext2, Ext3, FreeBSD UFS/UFS2, Solaris UFS, QNX4, QNX6, MINIX, Ext4, ReiserFS (ТУ 26.20.40.140-102-37222406-2021, ТУ 26.20.40.140-108-37222406-2022 и ТУ 26.20.40.140-115-37222406-2023);

- FAT12, FAT16, FAT32, NTFS, Ext2, Ext3 Ext4, FreeBSD UFS/UFS2, QNX4, QNX6, XFS (ТУ 26.20.40.140-079-37222406-2019, ТУ 26.20.40.140-113-РДСУ-2023).

Комплекс СЗИ НСД для ПЭВМ (РС) «Аккорд-АМДЗ» обеспечивает:

– защиту ресурсов ПЭВМ (РС) от лиц, не допущенных к работе на ней, на основе идентификации пользователей ПЭВМ (РС) по персональным идентификаторам до загрузки операционной системы (ОС);

– аутентификацию пользователей ПЭВМ (РС) по паролю длиной до 12 символов[2)], вводимому с клавиатуры с защитой от раскрытия пароля - до загрузки операционной системы (ОС);

– блокировку загрузки с отчуждаемых носителей (FDD, CD/DVD-ROM, ZIP, USB-накопителей и др.);

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

[2)] Для моделей «Аккорд-АМДЗ» (ТУ 4012-038-11443195-2011, ТУ 26.20.40.140-079-37222406-2019 и ТУ 26.20.40.140-113-РДСУ-2023) версии 0.3.11.47 максимальное допустимое значение длины пароля – 63 символа.

– контроль целостности технических, программных средств, условно-постоянной информации ПЭВМ (РС) до загрузки ОС, с реализацией пошагового алгоритма контроля;

– контроль целостности объектов файловых систем, размещенных на динамических дисках;

– доверенную загрузку системного и прикладного ПО при одновременной установке на дисках или в логических разделах диска ПЭВМ (РС) нескольких ОС;

– регистрацию на ПЭВМ (РС) до 126 пользователей (для моделей на базе специализированных контроллеров «Аккорд-5.5(е)») и до 1022 пользователей на одной ПЭВМ (для моделей на базе специализированных контроллеров семейства «Аккорд-LE/GX»);

– регистрацию контролируемых событий в системном журнале, размещенном в энергонезависимой памяти контроллера;

– возможность физической коммутации управляющих сигналов периферийных устройств, в зависимости от уровня полномочий пользователя, позволяющей управлять вводом/выводом информации на отчуждаемые физические носители и устройства обработки данных (для моделей на базе специализированных контроллеров «Аккорд-5.5(е)»);

– администрирование встроенного ПО комплекса (регистрацию пользователей и персональных идентификаторов, назначение файлов для контроля целостности, контроль аппаратной части ПЭВМ (РС), просмотр системного журнала);

– регистрацию, сбор, хранение и выдачу данных о событиях, происходящих в ПЭВМ (РС) в части системы защиты от несанкционированного доступа.

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

При модификации системного ПО замена контроллера не требуется. При этом обеспечивается поддержка спецрежима программирования контроллера без снижения уровня защиты.

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

Комплекс СЗИ НСД «Аккорд-АМДЗ» разработан ОКБ САПР на основании лицензий ФСТЭК и ФСБ РФ. Комплекс производится на аттестованном производстве.

1.2. Состав комплекса

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

- специализированный контроллер (далее по тексту – контроллер);
- программное обеспечение (ПО), состоящее из резидентной и нерезидентной частей.

Модификация контроллера определяется размером и шинным интерфейсом.

Резидентная часть ПО комплекса размещается в энергонезависимой флэш-памяти специализированного контроллера и включает в себя:

а) системное программное обеспечение (СПО):

- ядро ОС Linux;
- штатный набор утилит для функционирования ОС Linux, работы комплекса на разных аппаратных платформах, функционирования аппаратной составляющей комплекса и персональных идентификаторов;
- резидентные драйверы специализированных контроллеров;
- резидентные драйверы персональных идентификаторов.

б) функциональное программное обеспечение (ФПО):

- 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).

СПО и ФПО комплекса на этапе изготовления изделия объединяются в единое резидентное ПО (firmware), которое хранится в энергонезависимой флэш-памяти специализированного контроллера.

Нерезидентная часть ПО комплекса устанавливается на ПЭВМ пользователя и включает в себя:

а) драйверы специализированных контроллеров для внешних операционных систем;

б) драйверы персональных идентификаторов для внешних операционных систем;

в) uefi-модуль контроллеров GXM2 v.P и GXM2 v.S (ТУ 26.20.40.140-079-37222406-2019).

Для удаленного управления специализированным контроллером (ТУ 26.20.40.140-102-37222406-2021) в состав комплекса может включаться дополнительное программное обеспечение, устанавливаемое как на серверную, так и на абонентскую часть комплекса.

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

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

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

1.3. Условия применения комплекса

Для установки комплекса «Аккорд-АМДЗ» требуется следующий минимальный состав технических и программных средств:

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

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

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

1.4. Организационные меры, необходимые для применения комплекса

Для эффективного применения средств защиты комплекса и поддержания необходимого уровня защищенности ПЭВМ (АС) и информационных ресурсов требуется:

- наличие администратора безопасности информации (супервизора; далее по тексту – Администратор БИ) – привилегированного пользователя, имеющего особый статус и абсолютные полномочия. Администратор БИ планирует защиту информации на предприятии (учреждении, фирме и т.д.), определяет права доступа пользователям в соответствии с утвержденным Планом защиты, организует установку комплекса в СВТ(РС), эксплуатацию и контроль правильности использования СВТ(РС) с внедренным комплексом «Аккорд», в том числе учет выданных идентификаторов, осуществляет периодическое тестирование средств защиты комплекса. Подробнее обязанности администратора БИ по применению комплекса изложены в документе «Руководство администратора»;
- разработка и ведение учетной и объектовой документации (инструкция администратора, инструкций пользователей, журнал учета идентификаторов и отчуждаемых носителей пользователей и др.). Все разработанные учетные и объектовые документы должны быть согласованы, утверждены у руководства и доведены до сотрудников (пользователей). Это необходимо для того, чтобы План защиты организации (предприятия, фирмы и т.д.) и действия СБИ (администратора БИ) получили юридическую основу;
- физическая охрана СВТ (АС) и ее средств, в том числе проведение мероприятий по недопущению изъятия контроллера комплекса;
- использование в СВТ (АС) технических и программных средств, сертифицированных как в Системе ГОСТ Р, так и в Государственной системе защиты информации (ГСЗИ);
- периодическое тестирование средств защиты комплекса.

2. Установка и настройка комплекса

Установка и настройка комплекса СЗИ НСД «Аккорд-АМДЗ» осуществляется администратором безопасности информации и описана в Руководстве по установке и Руководстве администратора.

3. Порядок работы на ПЭВМ с установленным комплексом

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

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

3.1. Выполнение контрольных процедур

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

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 БИ интервал времени;
- проверка ограничения на время входа оператора (пользователя) в систему.

3.1.1. Процедура идентификации оператора (пользователя)

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

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

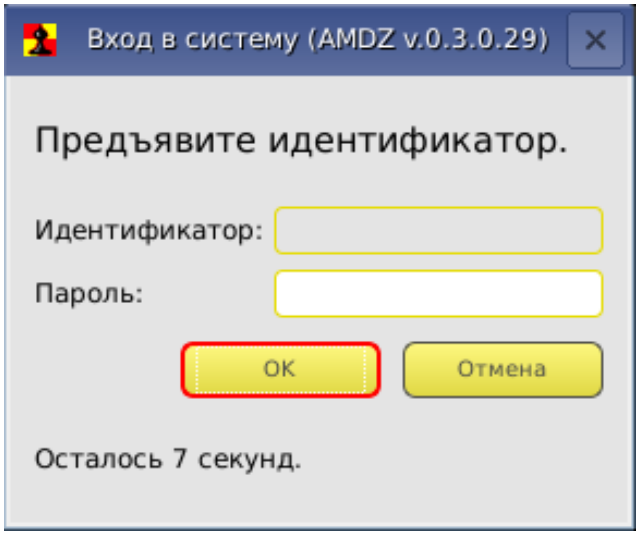

Рисунок 1 – Окно входа в систему с запросом идентификатора

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.

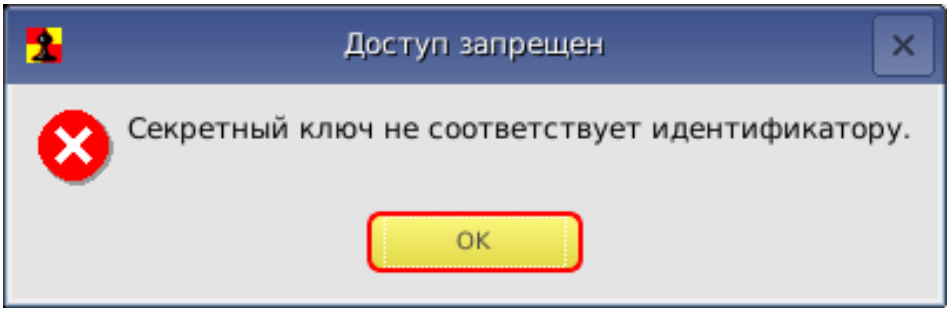

Рисунок 2 – Сообщение об ошибке

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. 3.1.2).

ВНИМАНИЕ! При авторизации на компьютере с «Аккорд-АМДЗ», поддерживающим режим загрузки BIOS UEFI, пользователи выполняют процедуру аутентификации только в текстовом интерфейсе, при этом ввод идентификатора возможен с клавиатуры (в случае, если последнее задано Администратором).

3.1.2. 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).

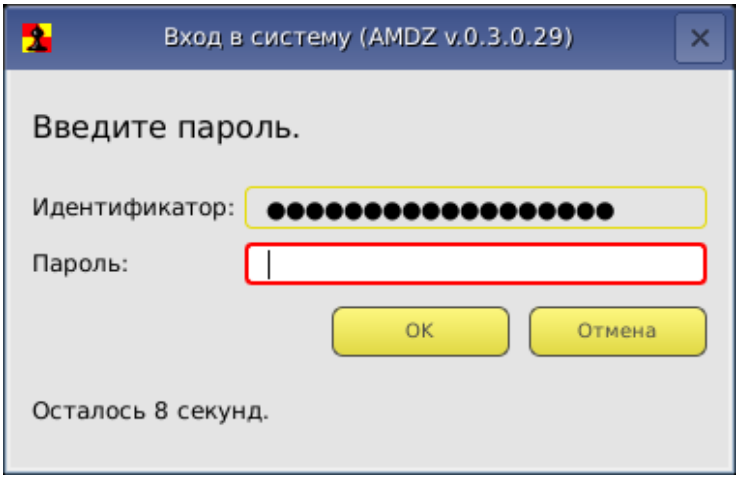

Рисунок 3 – Окно входа в систему с запросом на введение пароля

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

Начиная с 10 дней до истечения срока действия АИП АНП и/или пароля, а также начиная с 10 оставшихся попыток входа (как успешных, так и нет) после ввода пароля на экран выводится соответствующее предупреждающее сообщение (рисунки 4 - 6).

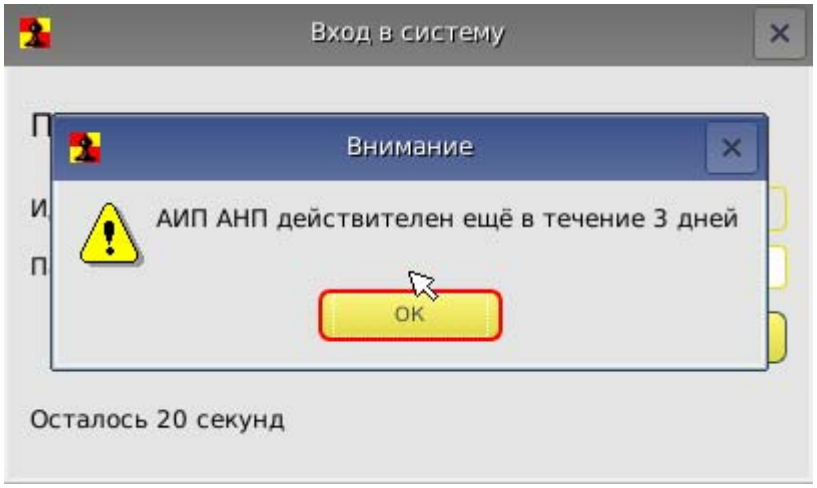

Рисунок 4 – Предупреждающее сообщение

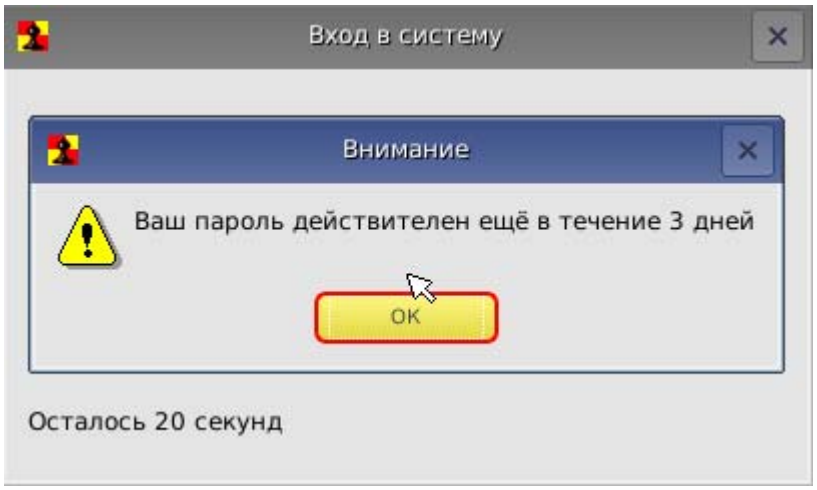

Рисунок 5 – Предупреждающее сообщение

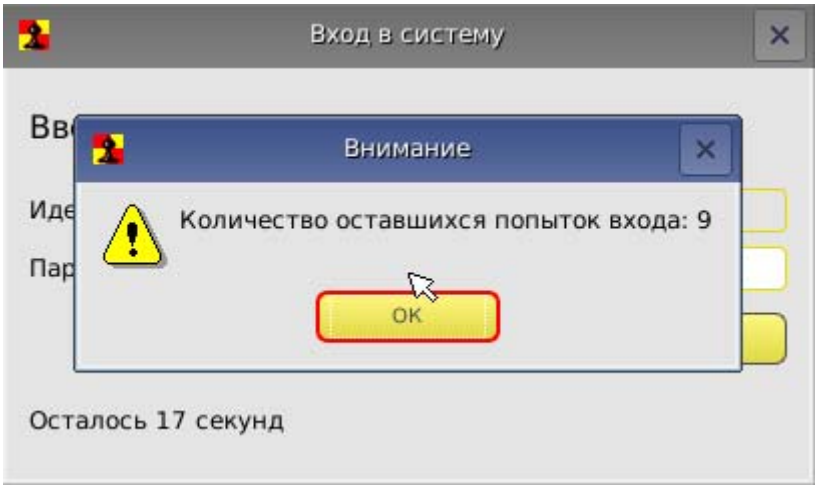

Рисунок 6 – Предупреждающее сообщение

После успешного завершения процедуры аутентификации контроллер переходит к следующему этапу – проверке целостности аппаратной части ПЭВМ (см. 3.1.3).

При неправильно введенном пароле на экран выводится соответствующее сообщение (рисунок 7) и оператору (пользователю) предлагается снова пройти процедуры идентификации и аутентификации (подтверждения достоверности).

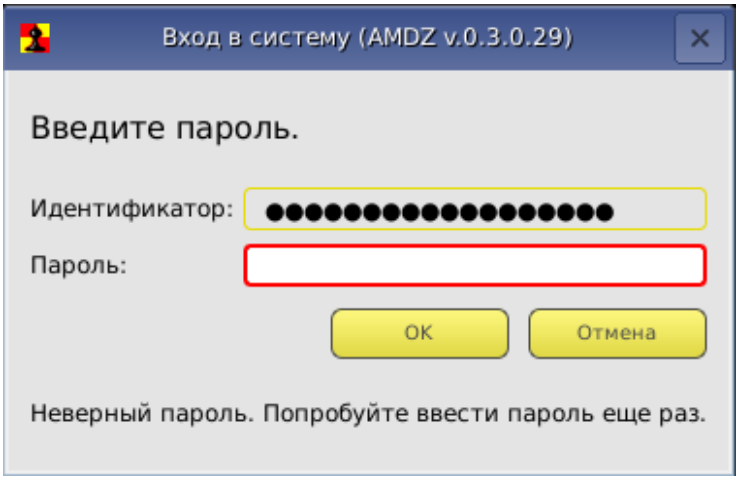

Рисунок 7 – Сообщение о неверно введенном пароле

Также на экран выводится диалоговое окно, сообщающее о количестве оставшихся неудачных попыток ввода пароля.

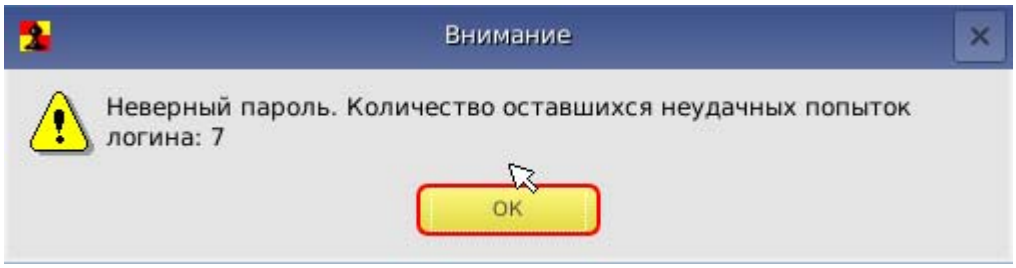

Рисунок 8 – Сообщение об оставшемся количестве неверных попыток ввода пароля

При превышении установленного администратором числа неверных попыток ввода пароля ПЭВМ блокируется. Продолжить работу можно только после перезагрузки ПЭВМ (рисунок 9).

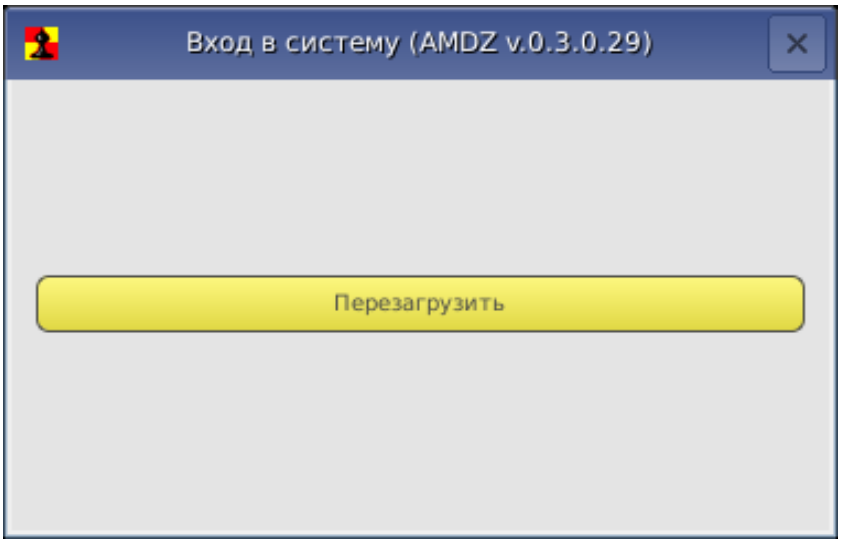

Рисунок 9 – Исчерпан лимит попыток идентификации

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 «Аккорд-АМДЗ», 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».

3.1.3. 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 10 (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.

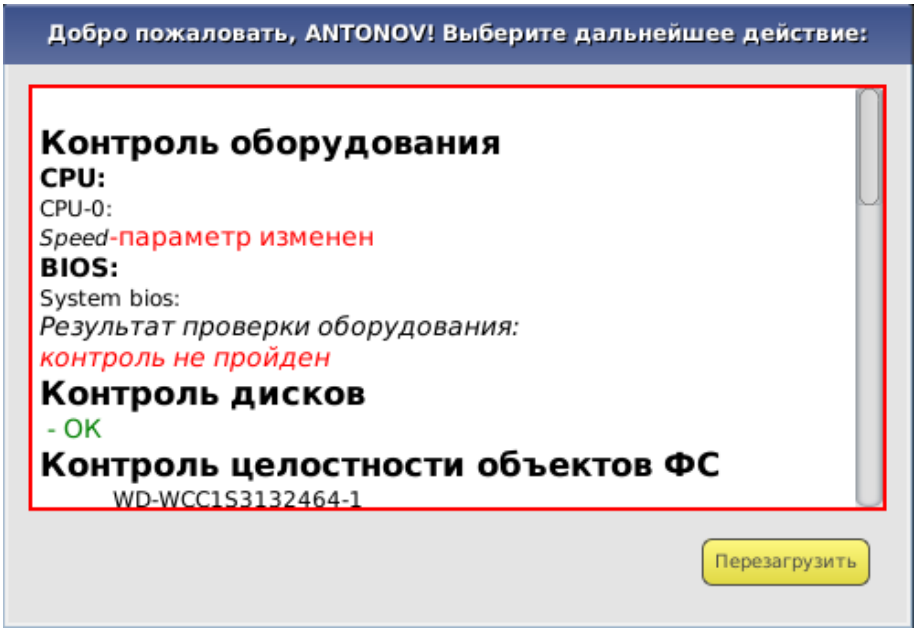

Рисунок 10 – Окно контроля целостности аппаратной части ПЭВМ

3.1.4. 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 БИ (входа в систему с помощью его персонального идентификатора).

3.1.5. Смена пароля по истечении срока его действия

Если время «жизни» пароля превысило отведенный интервал, 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 11. В таком случае для смены пароля необходимо обратиться к администратору БИ.

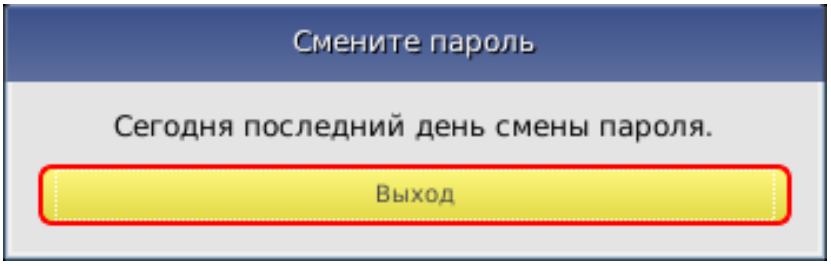

Рисунок 11 – Сообщение о необходимости смены пароля в случае, если пользователь (оператор) не обладает соответствующими правами

Если оператору (пользователю) предоставлено право самостоятельной смены пароля (для «Аккорд-АМДЗ», выпускаемых по ТУ 4012-038-11443195-2011, ТУ 26.20.40.140-079-37222406-2019 и ТУ 26.20.40.140-113-РДСУ-2023), при вводе просроченного пароля на экран выводится окно, показанное на рисунке 12.

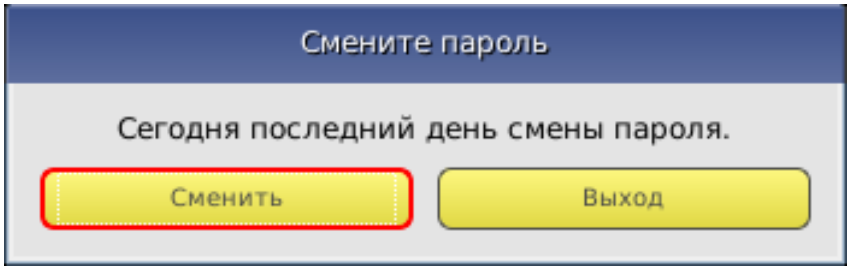

Рисунок 12 – Сообщение о необходимости смены пароля в случае если пользователь (оператор) обладает соответствующими правами

Для выполнения процедуры смены пароля следует нажать кнопку <Сменить>. На экран выводится окно смены пароля, показанное на рисунке 13.

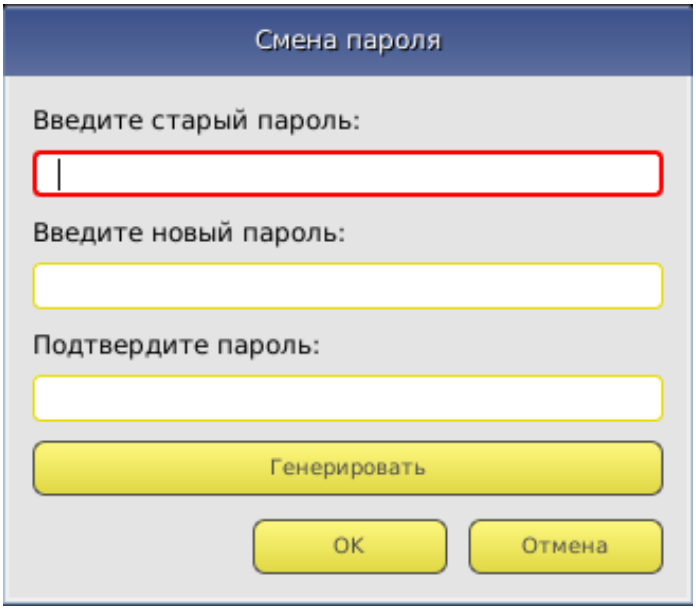

Рисунок 13 – Окно смены пароля

В данном окне необходимо ввести старый пароль, указать новый[3] 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.

Если новый пароль подтвержден правильно, 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, выводится сообщение, показанное на рисунке 14.

[3] 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.

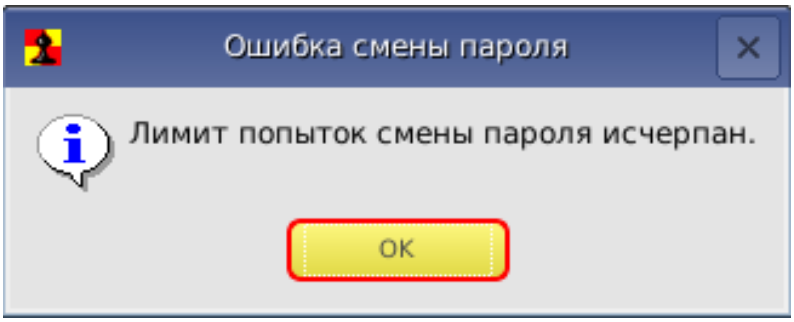

Рисунок 14 – Сообщение об исчерпании лимита попыток смены пароля

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.

3.1.6. 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. 3.1.5 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 13) выполнить процедуру смены пароля, описанную в п. 3.1.5 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 13) выполнить процедуру смены пароля, описанную в п. 3.1.5 настоящего Руководства.

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

Если администратор БИ 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 15.

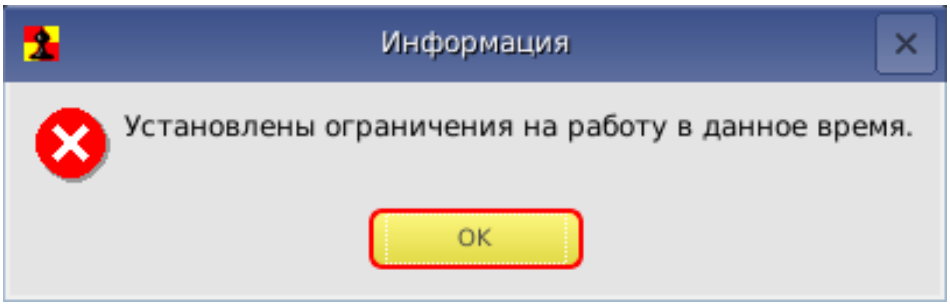

Рисунок 15 – Сообщение о наличии ограничений на работу в данное время

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

3.2. 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.

3.3. Завершение работы

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

4. О блокировке загрузки с отчуждаемых носителей

СЗИ НСД «Аккорд-АМДЗ» обеспечивает блокировку загрузки с отчуждаемых носителей.

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

5. 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 предъявить идентификатор (после появления на экране соответствующего запроса)
	В память идентификатора не записан секретный ключ пользователя	Убедиться в том, что в память идентификатора записан секретный ключ пользователя
«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 БИ. 2. Уточнить разрешенное время работы с учетом принятых ПРД. 3. Администратор БИ (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 БИ (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 БИ. 2. Сменить пароль с помощью администратора БИ.
«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.