ОКБ
ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

Программно-аппаратный комплекс защиты информации от НСД для ПЭВМ (PC)
«Аккорд-АМДЗ»
(Аппаратный модуль доверенной загрузки)

Руководство пользователя

11443195.4012.006 34 03

Листов 16

Москва
2014

АННОТАЦИЯ

Настоящий документ является руководством пользователя программно-аппаратного комплекса средств 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 приведено описание использования основных целевых функций комплексов СЗИ НСД «Аккорд-АМДЗ», работающих на основе контроллеров Аккорд-5MX, Аккорд-5.5, Аккорд-5.5e, Аккорд-5.5MP, Аккорд-5.5ME.

Особенности установки и управления комплексом приведены в документе «Руководство администратора» (11443195.4012.006 90 03).

Перед установкой и эксплуатацией комплексов 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 комплексов 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 – персональный идентификатор пользователя – микропроцессорное устройство DS1992 – DS1996 («Touch memory», далее по тексту – ТМ-идентификатор) или устройство ПСКЗИ ШИПКА.

Пользователь – субъект доступа к объектам (ресурсам) СВТ.

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

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

АМДЗ	Аппаратный модуль доверенной загрузки
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
ПСКЗИ	Персональное средство криптографической защиты информации
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

Комплекс СЗИ НСД «Аккорд-АМДЗ» представляет собой аппаратный модуль доверенной загрузки (АМДЗ) для IBM-совместимых ПК – серверов и рабочих станций локальной сети, обеспечивающий защиту устройств и информационных ресурсов от НСД, идентификацию, аутентификацию пользователей, регистрацию их действий, контроль целостности файлов и областей HDD (в том числе и системных) при многопользовательском режиме их эксплуатации.

Комплекс начинает работу сразу после выполнения кода системного BIOS компьютера – до загрузки операционной системы, и обеспечивает доверенную загрузку[1] ОС, использующих одну из поддерживаемых файловых систем. Это, в частности, ОС типа MS-DOS, ОС семейства Windows, QNX, OS/2, UNIX, LINUX, BSD и др.

Все модификации комплекса поддерживают файловые системы FAT12, FAT16, FAT32, NTFS, HPFS, Ext2, Ext3, FreeBSD UFS/UFS2, Solaris UFS, QNX4, MINIX.

Комплекс представляет собой совокупность технических и программных средств, предназначенных для выполнения основных функций защиты от НСД ПЭВМ (АС) на основе:

- применения персональных идентификаторов пользователей;
- парольного механизма;
- блокировки загрузки операционной системы со съемных носителей информации;
- контроля целостности технических средств и программных средств (файлов общего, прикладного ПО и данных) ПЭВМ (АС);
- обеспечения режима доверенной загрузки установленных на ПЭВМ (АС) операционных систем, использующих любую из поддерживаемых комплексом файловых систем.

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, вводимому с клавиатуры с защитой от раскрытия пароля - до загрузки операционной системы (ОС);

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

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

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

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

– регистрацию на ПЭВМ (PC) до 126 пользователей;

– 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;

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

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

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

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» включает в себя программные и аппаратные средства.

1.2.1. Аппаратные средства

Аппаратные средства ПАК СЗИ НСД «Аккорд-АМДЗ» (ТУ 4012-006-11443195-97 03) включают в себя:

– ***одноплатный контроллер*** - представляет собой карту расширения (expansion card), устанавливаемую в свободный слот материнской платы ПЭВМ (PC). Контроллер изготовлен по современной технологии многослойных печатных плат с покрытием химическим золотом с использованием наиболее современной элементной базы, является универсальным, не требует замены при смене используемого типа операционной системы (ОС). В контроллере комплекса аппаратно реализована работа с каналом Touch Memory, что обеспечивает надежную работу с идентификаторами DS-199x на всех типах ПЭВМ (PC). На контроллеры серии 5.5 по заказу может устанавливаться процессор с USB-хостом и разъем mini-USB, что позволяет использовать в качестве идентификатора ПСКЗИ ШИПКА.

– ***съемник информации с контактном устройством***, обеспечивающий интерфейс между контроллером комплекса и персональным идентификатором пользователя.

– ***персональный идентификатор пользователя*** – микропроцессорное устройство DS 199x («Touch memory»), или USB-устройство ПСКЗИ ШИПКА. Каждый идентификатор обладает уникальным номером (48 бит), который формируется технологически. Объем памяти, доступной для записи и чтения зависит от типа идентификатора.

Количество и тип идентификаторов, модификация контроллера и контактного устройства оговаривается при поставке комплекса и указываются в Формуляре (11443195.4012-006 ФО).

Порядок использования идентификаторов:

1) если в качестве персонального идентификатора пользователя используется ТМ-идентификатор:

- приложить ТМ-идентификатор пользователя к контактному устройству съемника информации;

2) если в качестве персонального идентификатора пользователя используется ПСКЗИ ШИПКА:

- подключить ПСКЗИ ШИПКА пользователя к USB-порту на плате контроллера (для контроллеров серии 5.5, имеющих установленный по заказу процессор с USB-хостом и разъем mini-USB).

1.2.2. Программные средства

В состав программных средств, размещенных в энергонезависимой памяти контроллера комплекса, входят:

1) BIOS контроллера комплекса «Аккорд-АМДЗ»;

2) программное обеспечение АМДЗ в составе следующих функциональных модулей:

– 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 аудита (работа с журналом регистрации событий);
- средства администрирования комплекса.

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

Программа администратора системы защиты информации является частью комплекса «Аккорд-АМДЗ» и не требует установки какого-либо дополнительного ПО. С помощью этой программы 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.

1.3. Технические условия применения комплекса

Все модификации комплекса «Аккорд-АМДЗ»:

- могут использоваться в составе ПЭВМ с центральным процессором архитектуры x86 (IA-32) или x86-64 (AMD64), с объемом динамической оперативной памяти (RAM) не менее 128 Мб, при наличии свободного разъема на материнской плате ПЭВМ, соответствующего типу специализированного контроллера АМДЗ;
- обеспечивают многопользовательский режим эксплуатации ПЭВМ с возможностью регистрации до 126 пользователей на одной ПЭВМ;
- предполагают наличие на ПЭВМ любой из ОС, использующей поддерживаемую комплексом файловую систему.

При модификации внутреннего ПО замена контроллера не требуется. При этом обеспечивается поддержка спецрежима (технологического режима контроллера) программирования без снижения уровня защиты.

Технические средства защищаемой ПЭВМ 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.

Обязанности администратора БИ по применению комплекса изложены в «Руководстве 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

Процедуры установки и настройки комплекса «Аккорд-АМДЗ» производятся администратором БИ и описаны в «Руководстве по установке» (11443195.4012-006 98/ 11443195.4012-038 98) и «Руководстве администратора» (11443195.4012.006 90 03) соответственно.

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.

К необязательным процедурам контроля относятся:

– проверка целостности системных областей диска и системного реестра;

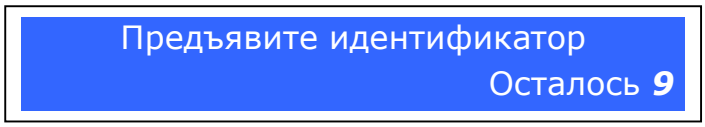
– проверка целостности программ и данных;

– 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)

При включении ПЭВМ, защищенной комплексом «Аккорд-АМДЗ», управление загрузкой передается контроллеру комплекса, при этом загружается программное обеспечение АМДЗ, после чего на экран выводится сообщение на синем фоне:



Сообщение остается на мониторе до момента контакта идентификатора пользователя и съемника информации. В правом нижнем углу окна выводится отсчет времени, отведенного пользователю для предъявления своего идентификатора. Если за отведенное время идентификатор не предъявлен, на экран выводится сообщение на красном фоне «Таймаут». Возобновить процедуру идентификации можно только после перезагрузки ПЭВМ.

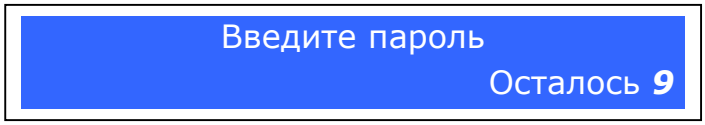
В случае если в память идентификатора не записан секретный ключ пользователя, или если пользователь недостаточно четко приложил персональный идентификатор к контактному устройству съемника информации, на экран выводится сообщение (на красном фоне), сопровождаемое звуковым сигналом:

и пользователю предлагается повторить процедуру идентификации.

При успешном завершении процедуры идентификации оператора (пользователя) происходит выполнение процедуры аутентификации (подтверждения достоверности), для чего на экран монитора выводится запрос на введение пароля пользователя.

3.1.2. Процедура аутентификации (подтверждение достоверности)

После идентификации оператора (пользователя), при условии, что ему при регистрации был задан пароль для входа в систему, на экран выводится сообщение на синем фоне:



По этой команде необходимо набрать свой личный пароль, при этом буквы пароля выводятся на экран в виде звездочек (*) и нажать клавишу <Enter>. Время, отведенное для ввода пароля, отображается в правом нижнем углу сообщения так же, как при запросе персонального идентификатора оператора (пользователя).

Если процедура аутентификации успешно завершилась, на экран выводится надпись на зеленом фоне:

Контроллер переходит к следующему этапу – проверке целостности аппаратной части ПЭВМ.

При неправильно введенном пароле на экран выводится надпись на красном фоне:

и оператору (пользователю) предлагается снова пройти процедуры идентификации и аутентификации (подтверждения достоверности). При троекратном неправильном вводе пароля ПЭВМ блокируется (выводится сообщение на красном фоне «Таймаут»). Продолжить работу можно только после перезагрузки ПЭВМ.

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, то в этом случае все равно происходит запрос пароля пользователя. После ввода пароля выводится сообщение «Доступ не разрешен!», а номер идентификатора заносится в системный журнал с пометкой «IID» (нелегальный идентификатор). Такой алгоритм работы СЗИ повышает надежность защитных функций комплекса – злоумышленник не может определить причину отказа в доступе.

3.1.3. Процедура контроля целостности аппаратной часта ПЭВМ

На этом этапе проводится проверка состава устройств, установленных на данной ПЭВМ. В случае, если нарушен состав аппаратной части ПЭВМ, выводится сообщение на красном фоне:

и загрузка ОС не производится. Загрузка будет возможна только после вмешательства администратора.

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 на целостность вычисляется контрольная сумма файлов и сравнивается с эталонным значением, хранящимся в контроллере. Эти данные заносятся при регистрации оператора (пользователя) и могут меняться в процессе эксплуатации ПЭВМ.

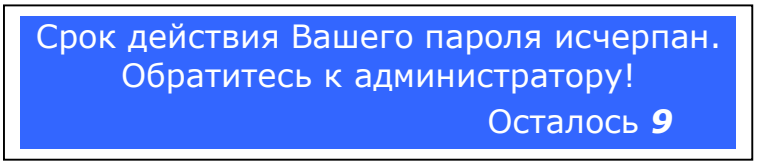
Если в ходе выполнения процедуры контроля целостности программной среды, обрабатываемой информации, системных областей и системных файлов нарушена целостность защищаемых файлов, выводится сообщение на красном фоне:

и загрузка ОС не производится. Загрузка будет возможна только после вмешательства администратора БИ (входом в систему с помощью его персонального идентификатора).

3.1.5. Смена пароля

Смена пароля выполняется в случае, когда время «жизни» пароля превысило отведенный интервал времени действия данного 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.

В случае, когда пользователь не имеет права на смену пароля, то при вводе просроченного пароля на экран выводится сообщение:



Если оператору (пользователю) предоставлено право самостоятельной смены пароля, то при вводе просроченного пароля на экран выводится сообщение:

где N – количество попыток для смены пароля, определяемое и устанавливаемое администратором БИ при регистрации оператора (пользователя).

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.

Далее необходимо ввести новый[1] пароль и нажать клавишу <Enter> - появляется окно с запросом для повторного ввода нового пароля:

Введите пароль еще раз

Следует повторно ввести новый пароль и нажать клавишу <Enter>. Если второй раз пароль введен правильно, то выводится сообщение «Новый пароль успешно установлен» и продолжается работа контроллера БК СЗИ НСД.

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

Не осталось попыток для смены пароля.
Обратитесь к администратору!
Осталось ***9***

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

Если оператору (пользователю) предоставлено право самостоятельной смены пароля, то он может сменить действующий пароль на новый в соответствии с правилами смены паролей. Эти правила должны быть оговорены в отдельной инструкции. Для смены пароля нужно после ввода старого пароля нажать не клавишу <Enter> (как при стандартном вводе пароля), а комбинацию клавиш <Ctrl>-<Enter>. Выполняется процедура смены пароля в соответствии с сообщениями, выводимыми на экран монитора, в порядке, указанном выше.

---

[1] пароль может состоять из букв, цифр и символов клавиатуры. 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.

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

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

Если оператору (пользователю) ПЭВМ запрещен вход в систему в данное время, то на экран выводится сообщение на красном фоне:

и загрузка операционной системы не выполняется. Порядок действий оператора (пользователя) в данной ситуации указан в таблице 1 (см. раздел 0 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, описанного в соответствующих руководствах.

4. 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 (499) 235-78-17, +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. Сообщения программных средств комплекса и порядок действий оператора

Таблица 1

Сообщение на экране	Причины появления сообщения	Порядок действий
«Ошибка чтения ТМ...» (на красном фоне)	Идентификатор был неправильно прислонен к контактному устройству съемника информации	Повторно приложить ТМ-идентификатор к контактному устройству съемника информации (после появления на экране соответствующего запроса)
«В данное время Вам работать не разрешается»	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 правил доступа. 3. Администратор БИ (при необходимости) должен установить разрешенный интервал времени для работы данного оператора (пользователя)
«Срок действия Вашего пароля исчерпан. Обратитесь к администратору для смены»	1. Окончилось время «жизни» установленного пароля. 2. Закончились все предоставленные попытки смены 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.
«Доступ не разрешен!» (на красном фоне)	1. Предъявлен незарегистрированный идентификатор. 2. Неправильно введен пароль	1. Предъявить зарегистрированный идентификатор и повторить процедуру идентификации. 2. Ввести правильный пароль. 3. При последующих неудачных попытках запуска ПЭВМ – обратиться к администратору БИ
«Требуется администратор!» (на красном фоне)	Несовпадение контрольных и текущих параметров аппаратной и программной частей ПЭВМ	1. Вызвать администратора БИ. 2. С помощью администратора БИ выявить и устранить причины изменения параметров.