

ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО



систем автоматизированного
проектирования

УТВЕРЖДЕН
11443195.4012- 006 -ЛУ

Программно-аппаратный комплекс средств защиты
информации от НСД для ПЭВМ (РС)
“Аккорд–АМДЗ”

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

11443195.4012-006 34 03

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ	3
2. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ И УСЛОВИЯ ПРИМЕНЕНИЯ	4
3. ПОРЯДОК РАБОТЫ НА ПЭВМ С УСТАНОВЛЕННЫМ КОМПЛЕКСОМ	5
3.1. ВЫПОЛНЕНИЕ КОНТРОЛЬНЫХ ПРОЦЕДУР	5
3.1.1. Процедура идентификации оператора (пользователя).....	5
3.1.2. Процедура аутентификации (подтверждение достоверности).....	6
3.1.3. Процедура контроля целостности аппаратной части ПЭВМ.....	6
3.1.4. Процедура контроля целостности системных областей, системных файлов, программ и данных.....	7
3.1.5. Смена пароля	7
3.1.6. Проверка ограничения на время входа оператора (пользователя) в систему.....	8
3.2. РАБОТА ОПЕРАТОРА (ПОЛЬЗОВАТЕЛЯ) В СООТВЕТСТВИИ С ФУНКЦИОНАЛЬНЫМИ ОБЯЗАННОСТЯМИ	9
3.3. ЗАВЕРШЕНИЕ РАБОТЫ	9
4. СООБЩЕНИЯ ПРОГРАММНЫХ СРЕДСТВ КОМПЛЕКСА И ПОРЯДОК ДЕЙСТВИЙ ОПЕРАТОРА	10

1. НАЗНАЧЕНИЕ

1.1. Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа для ПЭВМ (PC) "Аккорд-АМДЗ" (далее по тексту - комплекс СЗИ НСД или комплекс "Аккорд-АМДЗ") предназначен для применения на IBM-совместимых ПЭВМ (рабочих станциях ЛВС) в целях их защиты от несанкционированного доступа (НСД), идентификации, аутентификации пользователей, регистрации их действий, контроля целостности технических и программных средств (файлов общего, прикладного ПО и данных) ПЭВМ (PC), обеспечения режима доверенной загрузки в различных операционных средах (MS DOS, Windows 9x, Windows NT/2000/2003/XP/Vista, OS/2, UNIX), а также любых других ОС, использующих файловые системы FAT12, FAT16, FAT32, NTFS, HPFS, FreeBSD, EXT2FS при многопользовательском режиме эксплуатации ПЭВМ (рабочих станций ЛВС).

1.2. Комплекс представляет собой совокупность технических и программных средств, обеспечивающих выполнение основных функций защиты от НСД ПЭВМ (PC) 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 (PC);
- обеспечения режима доверенной загрузки установленных в ПЭВМ (PC) операционных систем, использующих любую из файловых систем: FAT12, FAT16, FAT32, NTFS, HPFS, FreeBSD, EXT2FS.

1.3. Программная часть комплекса, включает средства идентификации и аутентификации, средства контроля целостности технических и программных средств ПЭВМ (PC), средства регистрации действий пользователей, а также средства администрирования (настройки встроенного ПО) и аудита (работы с регистрационным журналом) и размещается в энергонезависимой памяти (ЭНП) контроллера при изготовлении комплекса.

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

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

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

1.5. 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.

2. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ И УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. 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);
- блокировку загрузки с отчуждаемых носителей (FDD, CD-ROM, Zip Drive);
- контроль целостности технических, программных средств, условно-постоянной информации ПЭВМ (РС) 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 (РС) нескольких ОС;
- поддержку файловых систем: FAT12, FAT16, FAT32, NTFS, HPFS, FreeBSd, EXT2FS;
- регистрацию на ПЭВМ (РС) 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 (РС), просмотр системного журнала);
- регистрацию, сбор, хранение и выдачу данных о событиях, происходящих в ПЭВМ (РС) в части системы защиты от несанкционированного доступа в ЛВС;

2.2. Комплекс СЗИ НСД "Аккорд-АМДЗ" применяется в ПЭВМ (РС) с процессором 80386 и выше, объемом RAM 1 Мбайт и более. Для установки контроллера комплекса требуется наличие свободного шинного разъема.

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

2.4. 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.

2.5. Для эффективного применения комплекса и поддержания необходимого уровня защищенности ПЭВМ (РС) и информационных ресурсов необходимы:

- физическая охрана ПЭВМ (РС) и их средств, в том числе проведение мероприятий по недопущению изъятия контроллера комплекса;
- наличие администратора безопасности информации (администратор БИ, либо АБИ) - привилегированного пользователя, имеющего особый статус и абсолютные полномочия (супервизора). Администратор БИ организует установку комплекса в ПЭВМ (РС), настройку защитных механизмов комплекса в соответствии с правами доступа пользователей, осуществляет контроль за правильным использованием ПЭВМ (РС) с установленным комплексом и периодическое тестирование средств защиты комплекса;
- учет выданных пользователям персональных идентификаторов;
- использование в ПЭВМ (РС) сертифицированных технических и программных средств.

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:

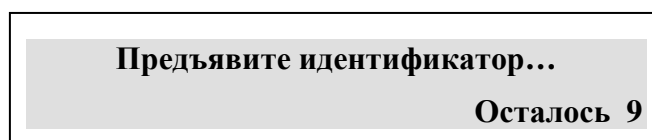
- процедура идентификации оператора (пользователя);
- процедура аутентификации (подтверждение достоверности) оператора (пользователя);
- контроль целостности аппаратной части ПЭВМ.

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 вверху экрана выводится сообщение: «Access system BIOS v.... copyright ОКВ SAPR ...», после чего на экран выводится сообщение на синем фоне:



Окно 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, то на экран выводится сообщение (на красном фоне), сопровождаемое звуковым сигналом:

Ошибка чтения идентификатора

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:

«Введите пароль»
Осталось 9

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:

«Доступ разрешен! »

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

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

«Доступ не разрешен!»

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 «ИТМ» (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 части 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:

**«Требуется Администратор.
Разберитесь с ошибками!»**

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:

**«Требуется Администратор.
Разберитесь с ошибками!»**

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:

**«Срок действия вашего пароля исчерпан.
Обратитесь к администратору !»**

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

**«Осталось N попыток для смены.
Новый пароль или ESC для отмены.»**

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 новый¹ пароль и нажать клавишу <Enter> - появляется окно с запросом для повторного ввода нового пароля:

Введите пароль еще раз

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 !»**

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.

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:

Вам запрещена работа в данное время!

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

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.

3.2. 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. СООБЩЕНИЯ ПРОГРАММНЫХ СРЕДСТВ КОМПЛЕКСА И ПОРЯДОК ДЕЙСТВИЙ ОПЕРАТОРА

При работе на ПЭВМ, оснащенной ПАК СЗИ НСД «Аккорд-АМДЗ», могут возникать ситуации, при появлении которых комплекс выдает сообщения.

Выводимые на экран монитора сообщения, причины их появления и порядок действий оператора (пользователя) по ним приведены в таблице 1.

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	<ol style="list-style-type: none"> 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)
«Срок действия Вашего пароля исчерпан. Обратитесь к администратору для смены»	<ol style="list-style-type: none"> 1. Окончилось время "жизни" установленного пароля. 2. Закончились все предоставленные попытки смены пароля. 	<ol style="list-style-type: none"> 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)	<ol style="list-style-type: none"> 1. Предъявлен незарегистрированный идентификатор. 2. Неправильно введен пароль. 	<ol style="list-style-type: none"> 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.	<ol style="list-style-type: none"> 1. Вызвать администратора БИ. 2. С помощью администратора БИ выявить и устранить причины изменения параметров.