

ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО



систем автоматизированного
проектирования

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН
11443195.4012-006 - ЛУ

**Программно-аппаратный комплекс средств защиты
информации от НСД для ПЭВМ (РС)**

“Аккорд–АМДЗ”

(Аппаратный модуль доверенной загрузки)

ОПИСАНИЕ ПРИМЕНЕНИЯ

11443195.4012-006 31 03

СОДЕРЖАНИЕ

АННОТАЦИЯ	3
ПРИНЯТЫЕ ТЕРМИНЫ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ	3
1. ОСНОВНЫЕ ПРИНЦИПЫ ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД И ОБЕСПЕЧЕНИЯ ЕЕ КОНФИДЕНЦИАЛЬНОСТИ.	4
2. НАЗНАЧЕНИЕ КОМПЛЕКСА.....	5
3. ХАРАКТЕРИСТИКА КОМПЛЕКСА.	6
4. УСЛОВИЯ ПРИМЕНЕНИЯ КОМПЛЕКСА.....	8
5. СОСТАВ КОМПЛЕКСА.	8
5.1. АППАРАТНЫЕ СРЕДСТВА.	8
5.2. ПРОГРАММНЫЕ СРЕДСТВА, РАЗМЕЩЕННЫЕ В ЭНП КОНТРОЛЛЕРА КОМПЛЕКСА.	9
6. ОСОБЕННОСТИ ЗАЩИТНЫХ ФУНКЦИЙ КОМПЛЕКСА.	9
7. ПОСТАВКА КОМПЛЕКСА	11
8. УСТАНОВКА И НАСТРОЙКА КОМПЛЕКСА	11
9. УПРАВЛЕНИЕ ЗАЩИТОЙ ИНФОРМАЦИИ.....	11
10. ПРАВОВЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ КОМПЛЕКСА	12
ЗАКЛЮЧЕНИЕ	12
ПРИЛОЖЕНИЯ.....	13
ФОРМИРОВАНИЕ И ПОДДЕРЖКА ИЗОЛИРОВАННОЙ ПРОГРАММНОЙ СРЕДЫ	13
МЕТОДИКА ОПРЕДЕЛЕНИЯ ТРЕБУЕМОЙ (ЦЕЛЕСООБРАЗНОЙ) ДЛИНЫ ПАРОЛЯ, ИСПОЛЪЗУЕМОГО В СЗИ НСД «АККОРД-АМДЗ» ПРИ АУТЕНТИФИКАЦИИ	16
АЛГОРИТМ ВЫЧИСЛЕНИЯ ХЭШ-ФУНКЦИИ, ПРИМЕНЯЕМЫЙ В СЗИ НСД «АККОРД-АМДЗ» ДЛЯ КОНТРОЛЯ ЦЕЛОСТНОСТИ ПС.....	17

АННОТАЦИЯ

Настоящий документ является описанием применения 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 приведены нормативные требования по защите информации, общие принципы и правила организации работы по обеспечению конфиденциальности информации, основные защитные функции комплекса, его возможности, особенности установки и применения.

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.

ПРИНЯТЫЕ ТЕРМИНЫ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Пользователь - субъект доступа к объектам (ресурсам) ПЭВМ.

Администратор БИ (или АБИ) - администратор безопасности информации, привилегированный пользователь - должностное лицо, имеющее особый статус и абсолютные полномочия (супервизора). Администратор БИ организует установку комплекса в ПЭВМ, настройку защитных механизмов комплекса в соответствии с правами доступа пользователей, осуществляет контроль за правильным использованием ПЭВМ с установленным комплексом и периодическое тестирование средств защиты комплекса.

идентификатор - персональный идентификатор пользователя (устройство DS1992 – DS1996, или ПСКЗИ ШИПКА).

Использовать идентификатор - приложить персональный идентификатор пользователя к контактному устройству съемника информации, или подключить к USB порту на плате контроллера.

Меню - окно с изображением кнопок с названиями команд. Перемещения по меню осуществляется с помощью клавиши <Tab>. Выбор команды - клавиша <Enter>, выход из меню - клавиша <Esc> или командой в меню.

Окно ввода/вывода - служит для ввода и отображения буквенно-цифровой информации, а так же может выполнять функции меню. Содержит окно для ввода буквенно-цифровой информации, окна списков, кнопки команд, окна флагов. Ввод буквенно-цифровой информации должен заканчиваться нажатием клавиши <Enter> или перемещением в другое окно, движение по пунктам списка в окне - с помощью клавиш <Стрелки>. Перемещение по окнам и кнопкам команд, выбор команд и выход из окна - аналогично работе с меню.

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

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

Пояснения - в описании некоторых команд даются пояснения и рекомендации администратору БИ для использования этих команд. Пояснения выделены мелким шрифтом.

1. ОСНОВНЫЕ ПРИНЦИПЫ ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД И ОБЕСПЕЧЕНИЯ ЕЕ КОНФИДЕНЦИАЛЬНОСТИ.

Мероприятия по защите информации от НСД являются составной частью управленческой, научной, производственной (коммерческой) деятельности предприятия (учреждения, фирмы и т.д.), независимо от его ведомственной принадлежности и формы собственности, и осуществляются в комплексе с другими мерами по обеспечению установленного режима конфиденциальности.

Практика организации защиты информации от НСД при ее обработке и хранении в АС должна учитывать следующие принципы и правила обеспечения безопасности информации:

1. Соответствие уровня безопасности информации законодательным положениям и нормативным требованиям по охране сведений, подлежащих защите по действующему законодательству, в т.ч. выбор класса защищенности АС в соответствии с особенностями обработки информации (технология обработки, конкретные условия эксплуатации АС) и уровнем ее конфиденциальности.

2. Выявление конфиденциальной информации и ее документальное оформление в виде перечня сведений, подлежащих защите, его своевременная корректировка.

3. Наиболее важные решения по защите информации должны приниматься руководством предприятия (организации, фирмы), владельцем АС.

4. Определение порядка присвоения уровня полномочий субъектам доступа, а также круга лиц, которым это право предоставлено.

5. Установление и оформление правил разграничения доступа (ПРД), т.е. совокупности правил, регламентирующих права доступа субъектов доступа к объектам доступа.

6. Установление личной ответственности пользователей за поддержание уровня защищенности АС при обработке сведений, подлежащих защите по действующему законодательству путем:

- ознакомления с перечнем защищаемых сведений, организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации;

- определения уровня полномочий субъекта доступа в соответствии с его должностным предназначением;

- получения от субъекта доступа расписки о неразглашении доверенной ему конфиденциальной информации.

7. Обеспечение физической охраны объекта, на котором расположена защищаемая АС (территория, здания, помещения, хранилища информационных носителей), путем установления соответствующих постов, технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими хищение средств вычислительной техники (СВТ), информационных носителей, а также НСД к СВТ и линиям связи.

8. Организация службы безопасности информации (ответственные лица, администратор АС), осуществляющей учет, хранение и выдачу информационных носителей, паролей, ключей, ведение служебной информации СЗИ НСД (генерацию паролей, ключей, сопровождение правил разграничения доступа), приемку включаемых в АС новых программных средств, а также контроль за ходом технологического процесса обработки конфиденциальной информации и т.д.

9. Плановый и оперативный контроль уровня безопасности защищаемой информации согласно НД по безопасности информации, в т.ч. проверка защитных функций средств защиты информации.

В н и м а н и е !

Средства защиты информации должны иметь СЕРТИФИКАТ, удостоверяющий их соответствие требованиям по безопасности информации.

2. НАЗНАЧЕНИЕ КОМПЛЕКСА.

Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа – *аппаратный модуль доверенной загрузки* – «Аккорд-АМДЗ» предназначен для применения на ПЭВМ (РС) типа **IBM PC** для защиты ПЭВМ (АС) и информационных ресурсов от НСД и контроля целостности файлов и областей HDD (в том числе и системных) при многопользовательском режиме их эксплуатации. При этом обеспечивается режим доверенной загрузки в различных операционных средах: MS DOS, Windows 3.x, Windows 95/98, Windows NT/2000/XP/Vista, OS/2, UNIX.

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 в ПЭВМ (АС) операционных систем, использующих любую из файловых систем: FAT 12, FAT 16, FAT 32, NTFS, HPFS, FreeBSD, Ext2FS, Sol86FS, QNXFS, MINIX.

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

* - под термином «доверенная загрузка» понимается загрузка ОС только после проведения контрольных процедур идентификации/аутентификации пользователей, проверки целостности технических и программных средств ПЭВМ (РС) с использованием алгоритма пошагового контроля целостности.

3. ХАРАКТЕРИСТИКА КОМПЛЕКСА.

Комплекс СЗИ НСД «Аккорд-АМДЗ» выпускается в программно-аппаратном исполнении и поставляется (по требованиям Заказчика) в различных модификациях.

Вся программная часть комплекса (включая средства администрирования), список пользователей и журнал регистрации размещены в энергонезависимой памяти контроллера. Этим обеспечивается возможность проведения идентификации/аутентификации пользователей, контроля целостности технических и программных средств ПЭВМ (PC), администрирования и аудита на аппаратном уровне, средствами контроллера комплекса до загрузки ОС.

В комплексе "Аккорд-АМДЗ" могут применяться различные модификации специализированных контроллеров:

- контроллер "Аккорд-5" используется для защиты ПЭВМ (PC) (PC) с шинным интерфейсом PCI;
- контроллер "Аккорд-5mx" используются для защиты ПЭВМ (PC) (PC) с шинным интерфейсом PCI (5B), или PCI-X (3.3B);
- контроллер "Аккорд-5.5" используются для защиты ПЭВМ (PC) (PC) с шинным интерфейсом PCI (5B), или PCI-X (3.3B);
- контроллер "Аккорд-5.5-Е" используются для защиты ПЭВМ (PC) (PC) с шинным интерфейсом PCI Express;

Характеристики контроллеров "Аккорд-АМДЗ" приведены в таблице 1.

Таблица 1. Модификации контроллеров «Аккорд-АМДЗ»

Особенности различных типов контроллеров	"Аккорд-5.5"	"Аккорд-5"	"Аккорд-5mx"
Тип используемой системной шины	PCI(5B) и PCI-X(3.3B)	PCI	PCI(5B) и PCI-X(3.3B)
Реле блокировки физических каналов	Три реле установлены по умолчанию	Возможна установка 2-х реле по заказу	Возможна установка 2-х реле по заказу
Возможность перепрограммирования	+	+	+
Таймер реального времени	Устанавливается по умолчанию	Возможна установка по заказу	Возможна установка по заказу
Аппаратный ДСЧ	Устанавливается на всех контроллерах		
Интерфейс RS 232	Устанавливается по умолчанию	Возможна установка по заказу	Возможна установка по заказу
Реле управления питанием материнской платы	Устанавливается по умолчанию	-	-
Встроенный USB-хост	Возможна установка по заказу	-	-

Все модификации комплекса "Аккорд-АМДЗ":

- могут использоваться на ПЭВМ с процессором **80486 и выше**, объемом **RAM** не менее **640 Кбайт**, при наличии свободного слота **PCI** на материнской плате ПЭВМ;
- используют для идентификации пользователей персональные идентификаторы TM DS 1992-1996, или ПСКЗИ ШИПКА модификаций 1.5, 1.6 и 2.0;
- используют для аутентификации пользователей пароль до **12** символов, вводимый с клавиатуры;
- блокируют загрузку с отчуждаемых носителей (**FDD, CD ROM, ZIP-drive**);
- обеспечивают контроль целостности аппаратных средств ПЭВМ (PC) до загрузки ОС;
- обеспечивают контроль целостности программ и данных до загрузки ОС, защиту от внедрения разрушающих программных воздействий (**РПВ**);
- поддерживают файловые системы следующих типов: FAT 12, FAT 16, FAT 32, NTFS, HPFS, FreeBSD, Ext2FS, Sol86FS, QNXFS, MINIX;

- осуществляют регистрацию действий пользователей в системном журнале, размещенном в энергонезависимой памяти контроллера;
- обеспечивают администрирование системы (регистрацию пользователей и персональных идентификаторов, назначение файлов для контроля целостности, контроль аппаратной части ПЭВМ, просмотр системного журнала);
- осуществляют разграничение прав доступа пользователей в соответствии с уровнем их полномочий (**при установке специального ПО**).

Для обеспечения разграничения доступа пользователей совместно с комплексом АМДЗ может поставляться (по отдельному заказу) специальное ПО:

v.1.95_00 – при работе ПЭВМ (PC) под управлением ОС Windows 9x;
NT/2000 v.3.0 – при работе ПЭВМ (PC) под управлением ОС Windows NT 4.0 (SP4-6)/2000/ XP/
Server 2000-2003/Vista.

Поставляемое совместно с комплексом «Аккорд-АМДЗ» специальное ПО реализует дискреционный и мандатный методы разграничения доступа и позволяет администратору безопасности информации (администратору БИ) описать правила разграничения доступа (ПРД) на основе наиболее полного набора атрибутов доступа.

а). При операциях с файлами:

- R** – разрешение на открытие файлов для чтения;
- W** – разрешение на открытие файлов для записи;
- C** – разрешение на создание файлов на диске;
- D** – разрешение на удаление файлов;
- N** – разрешение на переименование файлов и подкаталогов;
- O** – эмуляция разрешения на запись информации в файл, имеющий более низкий приоритет, чем атрибут **W** (разрешение на открытие файлов для записи).
- V** - видимость файлов. Позволяет делать существующие файлы невидимыми для пользователя. Атрибут **V** имеет более высокий приоритет, чем атрибуты **R, W, D, N, O**;

б). При операциях с каталогами:

- M** – разрешение на создание подкаталогов;
- E** – разрешение на удаление подкаталогов;
- n** – разрешение на переименование подкаталогов;
- G** – разрешение перехода в конкретный каталог (доступность каталога);

в). При операциях с программами (задачами):

- X** – разрешение на запуск программ;

г). Атрибуты принудительной регистрации:

- r** – всех операций чтения файла в журнале регистрации;
- w** – всех операций записи файла в журнале регистрации.

Мандатный механизм разграничения допускает установку для объектов меток доступа, а пользователям присвоение уровней доступа. Администратор БИ может описать и присвоить до 15 различных уровней.

Такой набор атрибутов позволяет реализовать любую разумную непротиворечивую политику информационной безопасности, обеспечить конфиденциальное делопроизводство.

4. УСЛОВИЯ ПРИМЕНЕНИЯ КОМПЛЕКСА.

Для установки комплекса “Аккорд-АМДЗ” требуется следующий минимальный состав технических и программных средств:

- IBM PC совместимая ПЭВМ, работающая под управлением операционной системы, поддерживающей любую из файловых систем FAT12, FAT16, FAT32, NTFS, HPFS, FreeBSD, Ext2FS;
- наличие свободного слота **PCI/PCI-X** на материнской плате **ПЭВМ**;
- при поставке совместно с комплексом специального ПО – объем дискового пространства для его размещения на жестком диске: для ПО **v.1.95** – около **3,0** Мбайт, для ПО **v. 3.0** – около 20 Мбайт.

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.

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

- физическая охрана ПЭВМ (АС) и ее средств с помощью технических средств, специального персонала, или других организационно-технических мер, в том числе проведение мероприятий по недопущению изъятия контроллера комплекса;
- наличие администратора безопасности информации (БИ) - привилегированного пользователя, имеющего особый статус и абсолютные полномочия. Обязанности администратора БИ по применению комплекса изложены в “**Руководстве администратора**”;
- учет носителей информации и идентификаторов пользователей;
- периодическое тестирование средств защиты комплекса "Аккорд";
- использование в ПЭВМ (АС) технических и программных средств, сертифицированных как в Системе **ГОСТ Р**, так и в **ГСЗИ**.

5. СОСТАВ КОМПЛЕКСА.

Комплекс СЗИ НСД «Аккорд-АМДЗ» включает программные и аппаратные средства.

5.1. Аппаратные средства.

- **Одноплатный контроллер** - представляет собой электронную плату, 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 переходе к другим типам 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 USB-хоста и разъем mini-USB, что позволяет использовать в качестве идентификатора ПСКЗИ ШИПКА.

- **Контактное устройство** – кабель интерфейса с идентификаторами пользователей типа DS 199x “Touch Memory, или ПСКЗИ ШИПКА.
- **Персональный идентификатор пользователей** – микропроцессорное устройство DS 199x (“Touch memory”), или ПСКЗИ ШИПКА в формате USB-устройства. Каждый идентификатор обладает уникальным номером (**48 бит**), который формируется технологически.

Количество и тип идентификаторов, модификация контроллера и контактного устройства оговаривается при поставке комплекса.

5.2. Программные средства, размещенные в ЭНП контроллера комплекса.

В состав программных средств входят:

- BIOS контроллера комплекса «Аккорд-АМДЗ»;
- 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

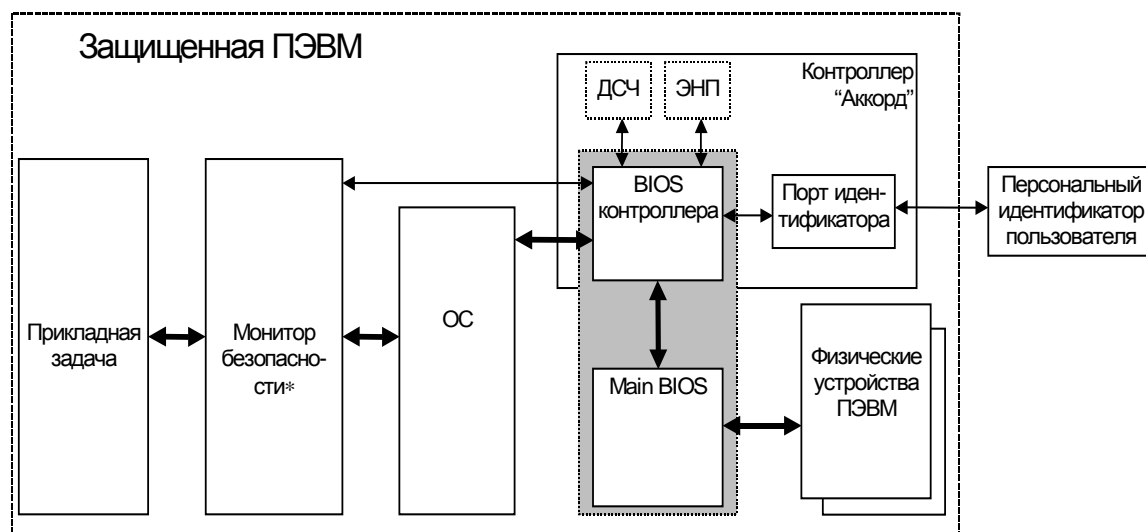
6. ОСОБЕННОСТИ ЗАЩИТНЫХ ФУНКЦИЙ КОМПЛЕКСА.

"Аккорд-АМДЗ" - это простой и чрезвычайно эффективный комплекс аппаратно - программных средств, позволяющий организовать без дополнительного ПО в составе ОС, «электронный замок» с функциями контроля целостности системных областей жесткого диска и прикладных программ (файлов) для любых распространенных типов файловых систем.

Защитные функции комплекса реализуются использованием:

1. Дисциплины защиты от НСД к ПЭВМ (PC), включая идентификацию пользователей по уникальному идентификатору и их аутентификацию (подтверждение подлинности) с учетом необходимой длины пароля, времени его жизни, ограничением времени доступа субъекта к ПЭВМ (PC).
2. Контроля целостности критичных с точки зрения информационной безопасности системных областей и файлов, программ и данных до загрузки ОС- **дисциплины защиты от несанкционированных модификаций и доверенной загрузки ОС.**
3. Других механизмов защиты в соответствии с нормативными документами по защите и требованиями Заказчика.

Построение системы защиты информации от НСД с использованием комплекса "Аккорд-АМДЗ" и его взаимодействие с программно-аппаратным обеспечением ПЭВМ (PC) показаны на рис 1.



* при установленном специальном ПО

Рис.1.

Надежность функционирования системы защиты ПЭВМ (PC) от НСД обеспечивается выполнением средствами СЗИ НСД «Аккорд-АМДЗ» следующих условий:

1. На ПЭВМ (PC) с проверенным BIOS установлена проверенная (сертифицированная) операционная система.
2. Достоверно установлена неизменность аппаратной части ПЭВМ, системного BIOS, критичных файлов ОС и прикладных программ для данного сеанса работы.
3. Кроме проверенных программ в данной программно-аппаратной среде ПЭВМ (PC) не запускалось и не запускается никаких иных программ.
4. Исключен запуск проверенных программ в какой-либо иной ситуации, т.е. вне проверенной среды – при установленном специальном ПО СЗИ НСД.
5. Условия 1-4 выполняются в любой момент времени для всех пользователей, аутентифицированных защитным механизмом комплекса.

Особенностью СЗИ НСД «Аккорд-АМДЗ» является проведение процедур идентификации, аутентификации и контроля целостности до загрузки операционной системы. Это обеспечивается перехватом управления контроллером комплекса во время так называемой процедуры ROMscan, суть которой заключается в следующем:

В процессе начального старта после проверки основного оборудования BIOS ПЭВМ (PC) начинает поиск внешних ПЗУ в диапазоне С 800:0000÷E000:0000 с шагом в 8 К. Признаком наличия ПЗУ является наличие слова AA55H в первом слове проверяемого интервала. Если данный признак обнаружен, то в следующем байте содержится длина ПЗУ в страницах по 512 байт.

Затем вычисляется контрольная сумма всего ПЗУ, и если она корректна - будет произведен вызов процедуры, расположенной в ПЗУ со смещением 3. Такая процедура обычно используется для инициализации BIOS плат расширения, установленных в ПЭВМ.

В СЗИ НСД «Аккорд-АМДЗ» в этой процедуре проводится инициализация внутреннего BIOS'а контроллера, перехват точки загрузки и возврат в процедуру ROMscan. Такой алгоритм обеспечивает корректную инициализацию всех устройств ПЭВМ. После завершения процедуры ROMscan управление передается на точку загрузки, и вот здесь уже начинает выполняться программа, записанная в энергонезависимой памяти контроллера. Стартует собственная ОС СЗИ «Аккорд АМДЗ», выполняются идентификация, аутентификация пользователя, контроль аппаратуры и файлов на жестком диске. При попытке НСД, или нарушении целостности возврат из процедуры не происходит, т.е. дальнейшая загрузка выполняться не будет. Внутреннее ПО контроллера также исключает возможность загрузки ПЭВМ со сменных носителей (флоппи-диск, CD ROM, ZIP-drive) для пользователей, не входящих в группу администраторов.

После предъявления персонального идентификатора производится аутентификация пользователя. Полученные данные служат основой для вычисления хеш-функции, и по этому значению осуществляется поиск в списке зарегистрированных пользователей, который хранится в ЭНП контроллера. Если пользователь зарегистрирован в контроллере АМДЗ, то выполняется контроль целостности установленных в ПЭВМ (PC) технических и программных средств по списку, созданному администратором БИ.

Для проведения процедуры аутентификации предусмотрен режим отображения пароля в скрытом виде при вводе - в виде символов <*>. Этим затрудняется возможность раскрытия личного пароля и использования утраченного (похищенного) идентификатора.

Основой для достижения надежного функционирования системы защиты является контроль целостности технических и программных средств ПЭВМ (PC) перед каждым сеансом работы пользователя. Этим обеспечивается защита от несанкционированных модификаций и внедрения разрушающих программных воздействий (закладок, вирусов и т.д.).

Контроль целостности в СЗИ НСД «Аккорд-АМДЗ» выполняется на аппаратном уровне (средствами контроллера комплекса) с использованием алгоритма пошагового (ступенчатого) контроля целостности (более подробно – см. Приложение 1.), суть которого сводится к следующему - для контроля данных на *i*-м логическом уровне их представления для чтения требуется использование предварительно проверенных на целостность процедур *i* - 1 - го уровня.

При этом обеспечивается корректная работа комплекса с загрузчиками различных файловых систем (Boot-менеджерами), что позволяет обеспечить доверенную загрузку всех ОС и прикладного ПО, при одновременной их установке на разных дисках или логических разделах дисков ПЭВМ (PC).

Программы, реализующие механизм контроля целостности комплекса, администрирования и аудит работы пользователей защищены от подделки и несанкционированной модификации за счет их хранения в области энергонезависимой памяти, которая защищена от записи.

7. ПОСТАВКА КОМПЛЕКСА

Комплекс СЗИ НСД “Аккорд-АМДЗ” для ПЭВМ (PC) поставляется в комплектности, соответствующей техническим условиям (ТУ 4012-006-11443195-97 03).

Модификация технических средств и специального программного обеспечения, поставляемого совместно с комплексом, оговаривается при заказе в соответствии с потребностями Заказчика и указывается в формуляре.

8. УСТАНОВКА И НАСТРОЙКА КОМПЛЕКСА

Установка комплекса осуществляется, как правило, специалистами **ЗАКАЗЧИКА (ПОТРЕБИТЕЛЯ)** в соответствии с требованиями эксплуатационной документации.

Установка комплекса СЗИ НСД "Аккорд-АМДЗ" включает:

1. Установку контроллера комплекса в свободный слот материнской платы ПЭВМ (PC) – см. "**Руководство по установке**" (11443195.4012-006 98 03).
2. Регистрацию пользователей и настройку защитных средств комплекса - см. "**Руководство администратора**" (11443195.4012-006 90 03).

9. УПРАВЛЕНИЕ ЗАЩИТОЙ ИНФОРМАЦИИ

Создаваемая структура защиты информации в ПЭВМ (АС) при применении комплекса СЗИ НСД "Аккорд-АМДЗ" должна поддерживаться механизмом установления полномочий пользователям ПЭВМ (АС) и управлением их доступом к информации.

Для этого на предприятии (учреждении, фирме и т.д.) создается служба безопасности информации (СБИ) или назначается ответственное лицо (администратор безопасности информации), на которых возлагается разработка и ввод в действие организационно-правовых документов по применению ПЭВМ (PC) с внедренными средствами защиты комплекса "Аккорд-АМДЗ". Этими документами предусматривается ведение ряда учетных и объектовых документов (например, “Журнал учета выданных идентификаторов”, “Инструкции по применению ПЭВМ с установленными комплексами СЗИ “Аккорд” для различных категорий должностных лиц и др.). В разработке необходимой документации ОКБ САПР может оказать необходимую помощь.

10. ПРАВОВЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ КОМПЛЕКСА

Программно-аппаратный комплекс "Аккорд-АМДЗ" и сопутствующая документация защищены законом России об авторских правах, а также положениями Международного Договора.

Любое использование данного комплекса в нарушение закона об авторских правах или в нарушение положений ЭД на комплекс "Аккорд-АМДЗ" будет преследоваться в установленном порядке.

Авторские права на программно-аппаратный комплекс СЗИ НСД «Аккорд-АМДЗ» и поставляемое с ним специальное ПО принадлежат **ОКБ САПР**

Разрешается делать архивные копии специального программного обеспечения комплекса "Аккорд-АМДЗ" для использования Потребителем, который приобрел комплекс в установленном порядке.

Ни при каких обстоятельствах поставляемое специальное программное обеспечение не распространяется между другими предприятиями (фирмами) и лицами.

Удалять в продукции ОКБ САПР уведомление об авторских правах не допускается ни при каких обстоятельствах.

При необходимости применения средств комплекса "Аккорд-АМДЗ" для других целей решение этого вопроса возможно только при наличии письменного согласия разработчиков.

Отметим, что предыдущие ограничения не запрещают легальным пользователям распространять собственные исходные коды или модули, связанные с применением специального ПО для комплекса "Аккорд-АМДЗ". Однако, тот, кто получает такие исходные коды или модули, должен приобрести собственную копию нашего специального ПО, чтобы на законном основании использовать его и иметь сертификат соответствия.

Относительно физических экземпляров аппаратуры и документации, поставляемых в составе комплекса "Аккорд-АМДЗ", **ОКБ САПР** гарантирует их исправность в соответствии с гарантийными обязательствами, указанными в Формуляре.

При обнаружении ошибок или дефектов пользователь направляет подробную рекламацию в ОКБ САПР в установленном порядке. При этом обязательным является наличие серийного номера на плате контроллера и формуляра на комплекс.

Комплекс "Аккорд-АМДЗ" поставляется по принципу "**as is**", т.е. владельцы авторских прав ни при каких обстоятельствах не предусматривают никакой компенсации за дополнительные убытки пользователя, включая любые потери прибыли, потери сохранности или другие убытки, вследствие аварийных ситуаций или их последствий, убытки, которые могут возникнуть из-за использования или невозможности использования нашей продукции.

При покупке и применении комплекса "Аккорд-АМДЗ" предполагается, что покупатель знаком с данными требованиями и согласен с положениями настоящего раздела.

ЗАКЛЮЧЕНИЕ

ОКБ САПР предлагает "горячую" линию для консультаций по телефонам **(495) 235-89-17** и **8-926-235-89-17** без дополнительной оплаты. Звоните нам по телефону поддержки с понедельника по пятницу с **10-00** до **18-00** (по московскому времени) по существу вопросов о применении комплекса "Аккорд-АМДЗ".



Россия, 113114, Москва, 2-ой Кожевнический пер. 8.



(495) 235.62.65/235.29.90, факс (495) 234.03.10, E-mail: 1@okbsapr.ru

Служба тех.поддержки: **E-mail: support@okbsapr.ru, 03@accord.ru**

Интернет: **WWW.ACCORD.RU**

ПРИЛОЖЕНИЯ.

Приложение 1.

Формирование и поддержка изолированной программной среды.

Предположим, что на ПЭВМ (PC) работают N субъектов-пользователей, каждый i -й из которых характеризуется некоторой персональной информацией K_i , не известной другим пользователям и хранящейся на некотором материальном носителе. Существует также выделенный субъект – администратор БИ, который знает все K_i . Администратор БИ присваивает i -му пользователю полномочия, заключающиеся в возможности исполнения им только заданного подмножества программ $T_i = \{Pi1, Pi2, \dots, Pit\}$.

Несанкционированным доступом является использование имеющихся на жестком диске ПЭВМ (PC) программ либо субъектом, не входящим в N допущенных, либо i -м пользователем вне подмножества своих полномочий T_i . Субъект, пытающийся проделать данные действия, называется злоумышленником. НСД осуществляется обязательно при помощи имеющихся на ПЭВМ (PC) или доставленных злоумышленником программных средств (в данном случае не рассматривается возможность нарушения целостности аппаратных средств ПЭВМ (PC)).

НСД может носить непосредственный и опосредованный характер. При непосредственном НСД злоумышленник, используя некоторое ПО пытается непосредственно осуществить операции чтения или записи (изменения) интересующей его информации. Если предположить, что в T_i нет программ, дающих возможность произвести НСД (это гарантирует администратор при установке полномочий), то НСД может быть произведен только при запуске программ, не входящих в T_i .

Опосредованный НСД обусловлен общностью ресурсов пользователей и заключается во влиянии на работу другого пользователя через используемые им программы (после предварительного изменения их содержания или их состава злоумышленником). Программы, участвующие в опосредованном НСД, будем называть *разрушающими программными воздействиями* (РПВ), или программными закладками.

РПВ могут быть внедрены i -м пользователем в ПО, принадлежащее j -му пользователю только путем изменения программ, входящих в T_j . Следовательно, система защиты от НСД ПЭВМ (PC) должна обеспечивать контроль за запуском программ, проверку их целостности и активизироваться всегда для любого пользователя. Выполнение контроля целостности и контроля запусков ведется на основе K_i для каждого пользователя.

При этом внедренный в ПЭВМ (PC) защитный механизм должен обеспечивать следующее:

- в некоторый начальный момент времени требовать у субъекта предъявления аутентифицирующей информации и по ней однозначно определять субъекта и его полномочия T_i ,
- в течение всего времени работы i -го пользователя выполняются программы только из подмножества T_i ,
- невозможность изменения пользователем подмножества T_i и/или исключения из дальнейшей работы защитного механизма, или его отдельных частей.

Предположим, что в ПЗУ (BIOS) и операционной среде, в том числе и в сетевом ПО, установленном на ПЭВМ (PC), отсутствуют специально интегрированные в них возможности НСД.

Пусть пользователь ПЭВМ (PC) работает с программой, в которой также исключено наличие каких-либо скрытых возможностей (на ПЭВМ (PC) установлены проверенные программы). Потенциально злоумышленные действия могут быть такими:

1. Проверенные программы будут запускаться на другой ПЭВМ с другим BIOS и в этих условиях могут использоваться некорректно.

2. Проверенные программы будут использованы в аналогичной, но не проверенной операционной среде, в которой они также могут использоваться некорректно.

3. Проверенные программы используются на проверенной ПЭВМ и в проверенной операционной среде, но запускаются еще и не проверенные программы, потенциально несущие в себе возможности НСД.

Несанкционированный доступ в ПЭВМ (PC) гарантировано невозможен, если выполняются следующие условия:

У1. На ПЭВМ (PC) с проверенным BIOS установлена проверенная операционная среда;

У2. Достоверно установлена неизменность ОС и BIOS для данного сеанса работы;

У3. Кроме проверенных программ в данной программно-аппаратной среде не запускалось и не запускается никаких иных программ. Проверенные программы перед запуском контролируются на целостность;

У4. Исключен запуск проверенных программ в какой-либо иной ситуации, т.е. вне проверенной среды;

У5. Условия У1-4 выполняются в любой момент времени для всех пользователей, аутентифицированных защитным механизмом.

При выполнении перечисленных условий программная среда называется изолированной (далее будем использовать термин ИПС - *изолированная программная среда*).

Функционирование программ в изолированной программной среде (ИПС) существенно снижает требования к базовому ПО - ИПС контролирует активизацию процессов через операционную среду, контролирует целостность исполняемых модулей перед их запуском и разрешает инициирование процесса только при одновременном выполнении двух условий - принадлежности к разрешенным и неизменности. В таком случае от базового ПО требуется только:

1. Невозможность запуска программ помимо контролируемых ИПС событий.

2. Отсутствие в базовом ПО возможностей влиять на среду функционирования уже запущенных программ (фактически, это требование невозможности редактирования оперативной памяти).

Все прочие действия, являющиеся нарушением У1-3, в оставшейся их части будут выявляться и блокироваться. Таким образом, ИПС существенно снижает требования к ПО в части наличия скрытых возможностей.

Основным элементом поддержания изолированности среды является контроль целостности. При этом возникает проблема чтения реальных данных, так как контроль целостности всегда сопряжен с чтением данных (по секторам, по файлам и т.д.). В процессе чтения РПВ может навязывать вместо одного сектора другой или редактировать непосредственно буфер памяти.

С другой стороны, даже контроль самого BIOS может происходить "под наблюдением" какой-либо дополнительной программы ("теневого BIOS") и не показывать его изменения. Аналогичные эффекты могут возникать и при обработке файла.

Таким образом, внедренное в систему РПВ может влиять на процесс чтения-записи данных на уровне файлов или на уровне секторов и предъявлять системе контроля некоторые другие, вместо реально существующих, данные. Этот механизм неоднократно реализовывался в STEALTH-вирусах.

Однако верно утверждение - если программный модуль, обслуживающий процесс чтения данных, не содержал РПВ и целостность его зафиксирована, то при его последующей неизменности чтение с использованием этого программного модуля будет

чтением реальных данных. Из данного утверждения следует способ ступенчатого контроля целостности.

Алгоритм ступенчатого контроля для создания ИПС (на примере DOS)

При включении питания ПЭВМ (PC) происходит тестирование оперативной памяти (ОП), инициализация таблицы прерываний и поиск расширений BIOS. При их наличии управление передается на них. После отработки расширений BIOS в память считывается первый сектор дискеты или винчестера (загрузчик) и управление передается на него, код загрузчика считывает драйверы DOS, далее выполняются файлы конфигурации, подгружается командный интерпретатор и выполняется файл автозапуска.

С учетом этого механизма для реализации ИПС предварительно фиксируется неизменность программ в основном и расширенных BIOS, далее, используя функцию чтения в BIOS (для DOS int 13h), читаются программы обслуживания чтения (драйверы DOS), рассматриваемые как последовательность секторов и фиксируется их целостность.

Далее, используя уже файловые операции, читаются необходимые для контроля исполняемые модули (командный интерпретатор, драйверы дополнительных устройств, *.exe и *.com-модули и т.д.). При запуске ИПС таким же образом и в той же последовательности выполняется контроль целостности.

Этот алгоритм можно обобщить на произвольную программную среду. Для контроля данных на i -м логическом уровне их представления для чтения требуется использование предварительно проверенных на целостность процедур $i-1$ -го уровня.

В случае описанного механизма загрузки процесс аутентификации необходимо проводить в одном из расширений BIOS (чтобы минимизировать число ранее запущенных программ), а контроль запуска программ включать уже после загрузки DOS (иначе DOS определяет эту функцию на себя). При реализации ИПС на нее должна быть возложена функция контроля за запуском программ и контроля целостности.

**Методика определения требуемой (целесообразной) длины пароля, используемого в СЗИ
НСД «Аккорд-АМДЗ» при аутентификации**

Оценка требуемой длины пароля важна для того, чтобы правильно выбрать период смены паролей из предположения, что идентификатор пользователя может быть утрачен, а пользователь, по тем или иным причинам, не поставит об этом в известность администратора безопасности информации.

Пусть вероятность подбора пароля в результате трехмесячных регулярных попыток ввода не должна превышать **0,001**.

По формуле Андерсона (см.Хоффман Л. Современные методы защиты информации /Пер.с англ./ М.:Советское радио, 1980, -264с.)

$$4,32 * 10^{**4} * k(M/P) \leq A^{**S}, \text{ где:}$$

k - количество попыток в мин;

M - период времени воздействия в месяцах;

P - вероятность подбора пароля;

A - число символов в алфавите;

S - длина пароля.

Время на одну попытку при использовании комплекса "Аккорд" – не менее **7** сек., т.е.

$$k = 60/7 = 8,57$$

Для английского алфавита **A = 26** и **S = 7**:

$$1,11 * 10^{**9} \leq 8,03 * 10^{**9},$$

т.е. пароля длиной **7** символов достаточно для выполнения условия, а именно - если будет выбран пароль длиной в **7** символов, то в течение **3**-х месяцев вероятность подбора пароля будет не выше **0,001**.

Если выбирается длина пароля в **6** символов (**S = 6**), то выполняется неравенство:

$$3,7 * 10^{**8} * M \leq 3,089 * 10^{**8},$$

или **M ≤ 0,83**, т.е. при длине пароля **6** символов и регулярном тестировании в течении **25** дней вероятность подбора пароля составит не более **0,001**.

Алгоритм вычисления хэш-функции, применяемый в СЗИ НДС «Аккорд-АМДЗ» для контроля целостности ПС

В комплексе программно-технических средств защиты информации от НДС для ПЭВМ (РС) «Аккорд–АМДЗ» применяется специальный алгоритм вычисления хэш-функции контрольной суммы файлов, что исключает возможность необнаружения их модификации.

Схема, реализующая алгоритм хеширования, состоит из двух регистров W и H, управляющих друг другом.

Регистр W содержит 16 ячеек W[0],W[1],...,W[15], а регистр H - 17 ячеек H[0],H[1],...,H[16], каждая длиной 8 бит (один байт).

За один такт работы схемы ячейки регистров W и H сдвигаются в сторону младших номеров, а в ячейки W[15] и H[16] записывается соответственно:

$$W[15] = (W[0]^W[2]^W[8]^W[13]) + S(5, H[15])$$

$$H[16] = W[0] + S(3, H[0]) + f[k](H[1], H[6], H[16]) , где:$$

^ - сложение по модулю 2;

+ - сложение по модулю 256;

S(L,A) - циклический сдвиг байта A на L разрядов в сторону старших разрядов;

& - логическое поразрядное 'И';

| - логическое поразрядное 'ИЛИ';

$$f[0](A,B,C) = \{A \& [C \wedge 0xFF] \mid [C \& (B \wedge 0xFF)]\};$$

$$f[1](A,B,C) = [(A \& B) \mid (B \& C) \mid (A \& C)];$$

$$f[2](A,B,C) = (A \wedge B \wedge C);$$

Выбор функции определяется номером такта.

Кроме того, при сдвиге ячейки W[11] в ячейку W[10] происходит также циклический сдвиг содержимого этой ячейки на 1 разряд в сторону старших разрядов.

Текст разбивается на блоки длиной 16 байт. Эти блоки поступают по очереди на вход схемы и записываются в регистр W по байту в ячейку, начиная с W[0]. Если длина текста не кратна 16 (в байтах), то к концу текста дописываются один байт FF (в шестнадцатеричной записи), затем нулевые байты до длины, кратной 16 (если они нужны). Последний блок, поступающий на вход схемы, это блок в 16 байт, в котором записана длина исходного текста в байтах.