ОКБ ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

Утвержден
37222406.26.20.40.140.102 - ЛУ

Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-АМДЗ»

Описание применения

37222406.26.20.40.140.102 31

Листов 14

АННОТАЦИЯ

Настоящий документ является описанием применения программно-аппаратного комплекса защиты информации от несанкционированного доступа – аппаратного модуля доверенной загрузки – «Аккорд-АМДЗ», далее по тексту «Аккорд-АМДЗ» или «Комплекс», и предназначен для лиц, планирующих и организующих защиту информации с их использованием в системах и средствах информатизации на базе ПЭВМ.

В документе приведены 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 «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 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.

АС – автоматизированная система.

БИ – безопасность информации.

Идентификатор – персональный аппаратный идентификатор пользователя (устройство "Touch-memory" DS-199x).

Использовать идентификатор – приложить персональный идентификатор пользователя к контактному устройству съемника информации.

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.

НСД – несанкционированный доступ.

Окно ввода/вывода – служит для ввода и отображения буквенно-цифровой информации, а также 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.

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

Пользователь – субъект доступа к объектам (ресурсам) ПЭВМ.

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

ПРД – правила разграничения доступа.

РПВ – разрушающие программные воздействия.

СВТ – средства вычислительной техники.

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

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АМДЗ	Аппаратный модуль доверенной загрузки
АБИ	Администратор безопасности информации
АС	Автоматизированная система
ВСПО	Вспомогательное специальное программное обеспечение
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
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
ЭНП	Энергонезависимая память

1. Назначение комплекса

Программно-аппаратный комплекс защиты информации от несанкционированного доступа – аппаратный модуль доверенной загрузки – «Аккорд-АМДЗ» предназначен для применения на ПЭВМ (ПК) 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.

Комплекс представляет собой совокупность технических и программных средств, предназначенных для обеспечения защиты технических средств ПЭВМ и информации от НСД.

2. Характеристики комплекса

Комплекс «Аккорд-АМДЗ» выпускается в программно-аппаратном исполнении.

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.

Комплекс «Аккорд-АМДЗ» реализуется на основе специализированных контроллеров «Аккорд».

Комплекс «Аккорд-АМДЗ» может применяться на ПЭВМ типа IBM PC, серверов и рабочих станций, основанных на процессорах с архитектурой x86 (IA-32) или x86-64 (AMD64), объемом RAM не менее 128 MB, при наличии свободного разъема на материнской плате ПЭВМ, соответствующего типу используемого специализированного контроллера.

Основными функциями комплекса «Аккорд-АМДЗ» по защите от НСД к ПЭВМ и информационным ресурсам являются следующие:

- блокировка загрузки со сменных носителей (FDD, CD/DVD-ROM, ZIP, USB-накопителей и др.) для пользователей, не обладающих правами администраторов;
- блокировка прерывания контрольных процедур с клавиатуры;
- идентификация пользователей с использованием физического электронного изделия – персонального идентификатора;
- аутентификация (подтверждения достоверности) пользователей с использованием пароля длиной от 0 до 12 символов, вводимого с клавиатуры в виде, защищенном от раскрытия индивидуального пароля пользователя (в виде символов <*>);
- аппаратный контроль целостности состава оборудования компьютера, системных областей, файлов и каталогов в файловых системах FAT12, FAT16, FAT32, NTFS, HPFS, Ext2, Ext3, Ext4, FreeBSD UFS/UFS2, Solaris

UFS, QNX4, QNX6, MINIX, ReiserFS, выполняемый до загрузки операционной системы;

– аппаратный контроль целостности реестра ОС семейства Microsoft Windows;

– доверенная загрузка операционной системы, а также доверенная загрузка системного и прикладного ПО, в том числе при одновременной установке на дисках или в разделах диска ПЭВМ нескольких произвольных ОС, функционирующих с поддержкой представленных файловых систем;

– автоматическое ведение журнала регистрируемых событий на этапе доверенной загрузки операционной системы (в энергонезависимой флэш-памяти аппаратной части комплекса);

– администрирование АМДЗ (регистрация пользователей и их персональных идентификаторов, создание и удаление групп пользователей, генерация пароля пользователя и определение его параметров; назначение объектов для контроля целостности и режимов контроля, работа с журналом регистрации системных событий и действий пользователей) и разделение прав администраторов комплекса;

– задание временных ограничений на доступ пользователей к ПЭВМ (РС) в соответствии с установленным для них режимом работы;

– поддержка режима удаленного управления с серверной частью комплекса;

– интеграция с другими программно-аппаратными и программными комплексами СЗИ НСД семейства «Аккорд», СЗИ НСД других производителей.

3. Условия применения комплекса

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

– ПЭВМ типа IBM PC, сервер или рабочая станция, основанная на процессоре с архитектурой x86 (IA-32) или x86-64 (AMD64), функционирующая под управлением операционной системы, поддерживающей любую из файловых систем FAT12, FAT16, FAT32, NTFS, HPFS, Ext2, Ext3, FreeBSD UFS/UFS2, Solaris UFS, QNX4, QNX6, MINIX, Ext4, ReiserFS;

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

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

– физическая охрана ПЭВМ (АС) и ее оборудования 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 – привилегированного пользователя, имеющего особый статус и абсолютные полномочия. Обязанности администратора БИ по применению комплекса

изложены в документе «Руководство администратора» (11443195.4012.038 90/11443195.4012.054 90/37222406.26.20.40.140.079 90/37222406.26.20.40.140.097 90/37222406.26.20.40.140.102 90);

– учет носителей информации и идентификаторов пользователей;

– периодическое тестирование средств защиты комплекса «Аккорд-АМДЗ».

4. Состав комплекса

Комплекс СЗИ НСД «Аккорд-АМДЗ» выпускается в программно-аппаратном исполнении.

4.1. Аппаратная часть

Аппаратная часть комплекса СЗИ НСД «Аккорд-АМДЗ» (ТУ 26.20.40.140-102-37222406-2021) включает в себя одноплатный контроллер - 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. Он является универсальным и не требует замены при переходе к другим типам ОС.

Контроллер комплекса «Аккорд-АМДЗ» (ТУ 26.20.40.140-102-37222406-2021) поддерживает работу со следующими типами персональных идентификаторов:

- ПАК «Персональный идентификатор ШИПКА»;
- DS-1993;
- DS-1996;
- Рутокен Lite;
- Рутокен S;
- Рутокен ЭЦП 2.0;
- Рутокен 2151;
- JaCarta-2 ГОСТ;
- eToken PRO (Java);
- ESMART® Token ГОСТ.

4.2. Программная часть

Программно-информационная часть комплекса, включающая программное обеспечение специализированного контроллера, базу данных зарегистрированных пользователей, список контролируемых объектов, журнал регистрации событий и средства администрирования, размещается в энергонезависимой флэш-памяти специализированного контроллера и включает в себя резидентную и нерезидентную составляющие.

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

– системное программное обеспечение (СПО), включающее в себя:

– 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.

– функциональное программное обеспечение (ФПО), реализующее комплекс мер по защите информации от НСД.

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

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

– драйверы специализированных контроллеров для внешних операционных систем;

– драйверы персональных идентификаторов для внешних операционных систем.

Для удаленного управления специализированным контроллером в состав комплекса может включаться дополнительное программное обеспечение, устанавливаемое как на серверную, так и на абонентскую часть комплекса. При этом под управлением одного сервера может находиться больше одного контроллера.

Состав дополнительного ПО серверной части комплекса:

- программное обеспечение системы удаленного централизованного управления средств защиты информации «Аккорд» (далее – ПО РАУ);

- базы настройки пользователей, аппаратных идентификаторов и специализированных контроллеров АПМДЗ.

Состав дополнительного ПО абонентской части комплекса:

- программное обеспечение средства криптографической защиты информации абонентской части (абонентское ПО СКЗИ), обеспечивающее криптографическую защиту канала связи с серверной частью;

- программное обеспечение для ОС Windows, обеспечивающее обмен данными с серверной частью СЗИ МДЗ «Аккорд-АМДЗ»;

- программное обеспечение для ОС Linux, обеспечивающее обмен данными с серверной частью СЗИ МДЗ «Аккорд-АМДЗ».

Для обеспечения криптографической защиты данных, передаваемых между серверной и абонентской частями комплекса, используется стороннее СКЗИ (например, КриптоПро CSP или DCrypt).

5. 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:

- 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);
- 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;
- других механизмов защиты в соответствии с нормативными документами по защите и требованиями Заказчика.

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

- достоверно установлена неизменность аппаратной части ПЭВМ, системного BIOS, критичных файлов ОС и прикладных программ для данного сеанса работы;
- кроме проверенных программ в данной программно-аппаратной среде ПЭВМ (PC) не запускалось и не запускается никаких иных программ;
- исключен запуск проверенных программ в какой-либо иной ситуации, т.е. вне проверенной среды – при установленном специальном ПО СЗИ НСД.

Эти условия 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 в течение так называемой процедуры ROM Scan, суть которой заключается в следующем:

В процессе начального старта после проверки основного оборудования BIOS ПЭВМ (PC) начинает поиск внешних ПЗУ в диапазоне 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 ROM Scan. Такой алгоритм обеспечивает корректную инициализацию всех устройств ПЭВМ. После завершения процедуры ROM Scan 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 (FDD, CD/DVD-ROM, ZIP, USB-накопителей и др.) 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 (РС) 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 (РС) 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, 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.

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.

6. Поставка комплекса

Комплекс СЗИ НСД «Аккорд-АМДЗ» для ПЭВМ (РС) поставляется в комплектности, соответствующей техническим условиям ТУ 26.20.40.140-102-37222406-2021.

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

7. 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 (РС) 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.

8. Ограничения по применению комплекса

1. ПАК СЗИ НСД «Аккорд-АМДЗ» может использоваться в составе ПЭВМ с центральным процессором архитектуры x86 (IA-32) или x86-64 (AMD64), с объемом динамической оперативной памяти (RAM) не менее 128 MB, при наличии свободного разъема на материнской плате ПЭВМ, соответствующего типу контроллера АМДЗ. Типы контроллеров «Аккорд-АМДЗ» с соответствующими им шинными интерфейсами на материнской плате ПЭВМ представлены в таблице 1. Расположение элементов и разъемов на платах контроллеров «Аккорд» различных модификаций см. в «Руководстве по установке» (11443195.4012.006 98/ 11443195.4012.038 98/ 11443195.4012.054 98/ 37222406.26.20.40.140.079 98/ 37222406.26.20.40.140.097 98/ 37222406.26.20.40.140.102 90).

Таблица 1 - Типы контроллеров «Аккорд-АМДЗ»

Шинный интерфейс слота СВТ	Тип контроллера
PCI-express	Аккорд-GX
mini PCI-express	Аккорд-GXMH
M2	Аккорд-GXM2
PCI-express	Аккорд-GX (исполнение 2)

2. ПАК СЗИ НСД «Аккорд-АМДЗ» предполагает наличие на ПЭВМ любой из ОС, поддерживающей файловые системы FAT12, FAT16, FAT32, NTFS, HPFS, Ext2, Ext3, Ext4, FreeBSD UFS/UFS2, Solaris UFS, QNX4, QNX6, MINIX, ReiserFS.

9. 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.

10. Техническая поддержка

В случае необходимости консультации АО «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) 762-17-72

или по адресу электронной почты help@okbsapr.ru.

Наш адрес в Интернете http://www.okbsapr.ru/.