ОКБ
ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

Утвержден
РДСУ.26.20.40.140.113 31 – ЛУ

Средство защиты информации от несанкционированного доступа «Аккорд-АМДЗ»

Описание применения

РДСУ.26.20.40.140.113 31

Листов 18

Москва
2023

АННОТАЦИЯ

Настоящий документ является описанием применения средства защиты информации от несанкционированного доступа – аппаратного модуля доверенной загрузки – «Аккорд-АМДЗ» (далее по тексту «Аккорд-АМДЗ», 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

1. Назначение комплекса 6
2. Характеристики комплекса 7
3. Условия применения комплекса 9
4. Состав комплекса 10
5. Особенности защитных функций комплекса 11
6. Поставка комплекса 13
7. Установка и настройка комплекса 14
8. Управление защитой информации 15
9. Ограничения по применению комплекса 16
10. Правовые аспекты применения комплекса 17
11. Техническая поддержка 18

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 СВТ, настройку защитных механизмов комплекса в соответствии с правами доступа пользователей, осуществляет контроль правильности использования СВТ с установленным комплексом и периодическое тестирование средств защиты комплекса.

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

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

Пользователь – субъект доступа к объектам (ресурсам) СВТ.

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

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 нормально 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
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
СКЦ	Список (списки) контроля целостности

1. Назначение комплекса

СЗИ НСД «Аккорд-АМДЗ» является программно-техническим средством, которое реализует функции по предотвращению несанкционированного доступа к программным и (или) техническим ресурсам средства вычислительной техники на этапе его загрузки в соответствии требованиями документов «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013), «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2018) и «Профиль защиты средства доверенной загрузки уровня платы расширения второго класса защиты. ИТ.СДЗ.ПР2.ПЗ» (ФСЭК России, 2013) при выполнении ограничений, указанных в ТУ 26.20.40.140-113-РДСУ-2023.

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

– несанкционированный доступ к информации за счет загрузки нештатной операционной системы (ОС) и обхода правил разграничения доступа штатной ОС и (или) других средств защиты информации, работающих в среде штатной ОС;

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

– нарушение целостности программного обеспечения средства доверенной загрузки;

– несанкционированное изменение конфигурации (параметров) средств доверенной загрузки;

– преодоление или обход функций безопасности средств доверенной загрузки.

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 Мбайт, при наличии свободного слота PCI-Express, miniPCI-Express или M2 (согласно типу используемого специализированного контроллера) на материнской плате ПЭВМ.

Комплекс начинает работу сразу после выполнения кода системного BIOS компьютера – до загрузки операционной системы, и обеспечивает доверенную загрузку[1].

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

- блокировка загрузки со съемных 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[2)], вводимого с клавиатуры в защищенном от раскрытия виде (в виде символов <*>);
- аппаратный контроль целостности состава оборудования компьютера, системных областей, файлов и каталогов, 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

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

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

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;
- 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 следующих файловых систем: FAT12, FAT16, FAT32, NTFS, Ext2, Ext3 Ext4, FreeBSD UFS/UFS2, QNX4, QNX6, XFS;
- 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»;
- 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 и включает:

- специализированный контроллер (далее по тексту – контроллер) с предустановленной на этапе изготовления резидентной операционной средой;
- функциональное программное обеспечение (далее по тексту - ФПО), работающее в резидентной операционной среде.

Резидентная операционная среда и ФПО на этапе изготовления комплекса объединяются в единое резидентное ПО (firmware) и размещаются в энергонезависимой флэш-памяти специализированного контроллера.

Модификация контроллера определяется размером и шинным интерфейсом. Резидентная операционная среда контроллера включает:

- резидентные драйверы специализированных контроллеров;
- резидентные драйверы персональных идентификаторов.

ФПО является ядром защиты и реализует комплекс мер по защите информации от НСД.

Состав резидентного программного обеспечения комплекса приведен в таблице 1.

Таблица 1 – Состав резидентного ПО

Компоненты	Состав	Назначение	Примечание
Резидентная операционная среда	Резидентные драйверы специализированных контроллеров и персональных идентификаторов	Среда функционирования ФПО	Изменение не влияет на функционал ядра защиты информации от НСД
ФПО	AMDZ-NG-GUI	Ядро защиты информации от НСД	При изменении необходимо проведение инспекционного контроля изделия

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:

1) Дисциплины защиты от НСД к ПЭВМ (РС), 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 (РС).

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.

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

1) Достоверно установлена неизменность аппаратной части ПЭВМ, системного BIOS, критичных файлов ОС и прикладных программ для данного сеанса работы.

2) Кроме проверенных программ в данной программно-аппаратной среде ПЭВМ (РС) не запускалось и не запускается никаких иных программ.

3) Исключен запуск проверенных программ в какой-либо иной ситуации, т.е. вне проверенной среды – при установленном специальном ПО СЗИ НСД.

4) Условия 1-3 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 ROM Scan, суть которой заключается в следующем:

В процессе начального старта после проверки основного оборудования BIOS ПЭВМ (РС) 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 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 съемных 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 при вводе пароля в скрытом виде - 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 ТУ 26.20.40.140-113-РДСУ-2023.

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

7. Установка и настройка комплекса

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

Установка и настройка комплекса СЗИ НСД «Аккорд-АМДЗ» включает:

1) Установку платы контроллера в свободный слот ПЭВМ – см. «Руководство по установке».

2) Регистрацию администратора БИ (супервизора), в том числе настройку комплекса в соответствии с конфигурацией технических средств ПЭВМ (подробнее см. «Руководство по установке» и «Руководство администратора», входящие в комплект поставки комплекса).

3) Регистрацию пользователей и настройку защитных средств комплекса – см. «Руководство администратора».

8. 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.

9. Ограничения по применению комплекса

1. 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 Мб, 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, а также расположение элементов и разъемов на платах контроллеров «Аккорд» различных модификаций см. в «Руководстве по установке».

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

3. Запрещается удаленное администрирование «Аккорд-АМДЗ» и взаимодействие с другими СЗИ по доверенным маршрутам при взаимодействии с уполномоченными субъектами.

10. Правовые аспекты применения комплекса

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 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.

11. 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/.