ОКБ АПР
ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

Утвержден
11443195.4012.006 31- ЛУ

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

Описание применения
11443195.4012.006 31

Листов 20

Москва

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, возможности, особенности установки и применения комплексов СЗИ НСД «Аккорд-АМДЗ», работающих на основе контроллеров:

- Аккорд-5MX, Аккорд-5.5, Аккорд-5.5e, Аккорд-5.5MP, Аккорд-5.5ME, Аккорд-LE, Аккорд-GX, Аккорд-GXM, Аккорд-GXMH, Аккорд-GXM2 (для СЗИ НСД «Аккорд-АМДЗ» с ФПО версии 0.3.x.y);
- Аккорд-GX, Аккорд-GXMH, Аккорд-GXM2 (для СЗИ НСД «Аккорд-АМДЗ» с ФПО версии 0.4.x.y).

Перед установкой и эксплуатацией комплексов СЗИ НСД «Аккорд-АМДЗ» необходимо внимательно ознакомиться с комплектом эксплуатационной документации.

Применение защитных средств комплексов должно дополняться общими мерами предосторожности и физической безопасности.

СОДЕРЖАНИЕ

ПРИНЯТЫЕ ТЕРМИНЫ И ОБОЗНАЧЕНИЯ

Администратор БИ (или АБИ) – администратор безопасности информации, привилегированный пользователь – должностное лицо, имеющее особый статус и абсолютные полномочия (супервизора). Администратор БИ планирует защиту информации на предприятии (учреждении, фирме и т.д.), определяет права доступа пользователям в соответствии с утвержденным Планом защиты, организует установку комплекса в СВТ, эксплуатацию и контроль правильности использования СВТ с внедренным комплексом «Аккорд», в том числе учет выданных идентификаторов, осуществляет периодическое тестирование средств защиты комплекса.

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

Идентификатор – 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.

Объект доступа – под объектом доступа понимается один из перечисленных ресурсов СВТ: диск, каталог, файл, процесс (задача).

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

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

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АМДЗ	Аппаратный модуль доверенной загрузки
АБИ	Администратор безопасности информации
АС	Автоматизированная система
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПК	Персональный компьютер
ПО	Программное обеспечение
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

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

Комплекс начинает работу сразу после выполнения кода системного BIOS компьютера – до загрузки операционной системы, и обеспечивает доверенную загрузку[1] ОС, поддерживающих файловые системы FAT12, FAT16, FAT32, NTFS, HPFS, Ext2, Ext3, FreeBSD UFS/UFS2, Solaris UFS, QNX4, MINIX.

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/DVD-ROM, ZIP, USB-накопителей и др.);
- 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;
- регистрацию на ПЭВМ (РС) до 126 пользователей (для моделей на базе специализированных контроллеров серии «Аккорд-5.5», «Аккорд-5MX») и до 1022 пользователей на одной ПЭВМ (для моделей на базе специализированных контроллеров семейства «Аккорд-LE/GX»);
- 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 (для

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

моделей на базе специализированных контроллеров серии «Аккорд-5.5», «Аккорд-5МХ»);

- 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.

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

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. Состав комплекса

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

2.1. Аппаратные средства

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

- ***одноплатный контроллер*** - представляет собой карту расширения (expansion card), устанавливаемую в свободный слот материнской платы ПЭВМ (РС). Контроллер является универсальным, не требует замены при смене используемого типа операционной системы (ОС).
- ***съемник информации с контактным устройством***, обеспечивающий интерфейс между контроллером комплекса и персональным идентификатором пользователя.
- ***персональный идентификатор пользователя.*** Каждый идентификатор обладает уникальным номером (48 бит), который формируется технологически. Объем памяти, доступной для записи и чтения, зависит от типа идентификатора. Подробнее о порядке использования персональных идентификаторов см. п. «Идентификаторы» «Руководства по установке» (11443195.4012.006 98/ 11443195.4012.038 98/ 11443195.4012.054 98), входящего в комплект поставки комплекса.

Количество и тип идентификаторов, модификация контроллера и контактного устройства оговариваются при поставке комплекса и указываются в Формуляре (11443195.4012.006 ФО).

Подробнее о контроллерах «Аккорд-АМДЗ», а также об устройствах, с которыми СЗИ НСД «Аккорд-АМДЗ» поддерживает работу, см. в документе «Руководство по установке», входящем в комплект поставки комплекса.

2.2. Программные средства

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

1) BIOS контроллера комплекса «Аккорд-АМДЗ»;

2) программное обеспечение АМДЗ в составе следующих функциональных модулей:

- средства идентификации пользователей;
- средства аутентификации пользователей;
- средства контроля целостности технических средств ПЭВМ (РС);
- средства контроля целостности системных областей жесткого диска;
- средства контроля целостности программных средств;
- средства контроля целостности отдельных ветвей реестра (для ОС семейства Windows);
- средства аудита (работа с журналом регистрации событий);
- средства администрирования комплекса (среда администрирования).

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

Среда администрирования является частью комплекса «Аккорд-АМДЗ» и не требует установки какого-либо дополнительного ПО. С помощью этой нее администратор СЗИ может добавлять и удалять пользователей, назначать пользователям идентификаторы и пароли, контролировать аппаратную часть ПЭВМ, прикладные и системные файлы, получает доступ к системному журналу контроллера.

3. Характеристика комплекса

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

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

Комплекс СЗИ НСД «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 (РС), администрирования и аудита на аппаратном уровне, средствами контроллера комплекса до загрузки ОС.

В комплексе «Аккорд-АМДЗ» могут применяться различные модификации специализированных контроллеров.

Типы контроллеров «Аккорд-АМДЗ» с соответствующими им шинными интерфейсами СВТ, представлены в таблице 1.

Таблица 1 - Типы контроллеров «Аккорд-АМДЗ»

Шинный интерфейс слота СВТ	Тип контроллера
PCI (с напряжением питания шины 5В или 3.3В) или PCI-X (с напряжением питания шины 3.3В)	Аккорд-5MX
	Аккорд-5.5
PCI-express	Аккорд-5.5.e
	Аккорд-LE
	Аккорд-GX
mini PCI	Аккорд-5.5MP
mini PCI-express	Аккорд-5.5ME
	Аккорд-GXM
	Аккорд-GXMH
M.2 с ключами A и/или E (интерфейс PCI-express)	Аккорд-GXM2

Расположение элементов и разъемов на платах контроллеров «Аккорд» различных модификаций см. в «Руководстве по установке» (11443195.4012.006 98).

4. 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, приведенных в подразделе **Ошибка! Источник ссылки не найден.** настоящего руководства;
- наличие на материнской плате ПЭВМ свободного слота PCI/PCI-Express/miniPCI-Express/M.2 – в соответствии с типом специализированного контроллера.

Технические средства защищаемой ПЭВМ не должны содержать аппаратно-программных механизмов, ориентированных на целенаправленное нарушение правильности функционирования комплекса. В составе ПЭВМ (РС), в котором установлен комплекс СЗИ НСД, должны отсутствовать средства, позволяющие за счет воздействия со стороны пользователей на штатные органы управления ПЭВМ (РС) воспрепятствовать передаче управления комплексу стандартной процедурой ROM Scan.

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 11443195.4012.006 90 «Руководство администратора»;
- учет носителей информации и идентификаторов пользователей;

периодическое тестирование средств защиты комплекса «Аккорд-АМДЗ».

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, включая возможность контроля целостности журнала транзакций NTFS, EXT3 и EXT4, 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)На ПЭВМ (РС) 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 (РС) 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 ROM Scan, суть которой заключается в следующем:

В процессе начального старта после проверки основного оборудования BIOS ПЭВМ (РС) 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 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 (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.

6. Поставка комплекса

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

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» (11443195.4012.006 98).

2) Настройку параметров учетной записи «Гл.Администратор», 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» (11443195.4012.006 90).

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. 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 ЗАО «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) 235-89-17

+7 (926) 762-17-72

или по адресу электронной почты help@okbsapr.ru.

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

Приложение 1. Формирование и поддержка изолированной программной среды

Предположим, что на ПЭВМ (PC) работают N субъектов-пользователей, каждый i-й из которых характеризуется некоторой персональной информацией Ki, не известной другим пользователям и хранящейся на некотором материальном носителе. Существует также выделенный субъект – администратор БИ, который знает все Ki. Администратор БИ присваивает i-му пользователю полномочия, заключающиеся в возможности исполнения им только заданного подмножества программ Ti={Pi1, Pi2, ... 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 Ti. 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 Ti нет программ, дающих возможность произвести НСД (это гарантирует администратор при установке полномочий), то НСД может быть произведен только при запуске программ, не входящих в Ti.

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 Tj. 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 Ki 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 Ti,
- в течение всего времени работы i-го пользователя выполняются программы только из подмножества Ti,

- невозможность изменения пользователем подмножества Ti 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 ("теневой BIOS") и не показать 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 STELTH-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.

Приложение 2. 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) <= A**S, 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 <= 8,03 * 10**9 ,

т.е. пароля длиной ***7*** символов достаточно для выполнения условия, а именно - если будет выбран пароль длинной 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 <= 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***.

Приложение 3. Алгоритм вычисления хэш-функции, применяемый в СЗИ НСД «Аккорд-АМДЗ» для контроля целостности ПС

В комплексе программно-технических средств защиты информации от НСД 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:

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

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

^ - 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 ^ 0xFF)] | [C & (B ^ 0xFF)]};

f[1](A,B,C) = [(A & B) | (B & C) | (A & C)];

f[2](A,B,C) = (A ^ B ^ 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.