Шахрай В.Н.,группа 019

ПРОГРАММНО-АППАРАТНАЯ ЗАЩИТА ИНФОРМАЦИИ НА БАЗЕ СЗИ НСД ”АККОРД”.

1. ДЛЯ ЧЕГО НУЖЕН «АККОРД».

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

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

Комплекс СЗИ НСД «Аккорд-АМДЗ» разработан ОКБ САПР на основании лицензий Гостехкомиссии России и ФАПСИ. Комплекс производится на аттестованном производстве.

2. ОБЕСПЕЧЕНИЕ РАЗГРАНИЧЕНИЯ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ.

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

v.1.35 – при работе ПЭВМ (PC) под управлением ОС MS DOS;
v.1.95 – при работе ПЭВМ (PC) под управлением ОС MS DOS, Windows 9x;
v.1.95_00 – при работе ПЭВМ (PC) под управлением ОС Windows 9x (с графическим интерфейсом);
v.2.0 – при работе ПЭВМ (PC) под управлением ОС Windows NT 4.0 (SP4-6)/2000/XP.

Поставляемое совместно с комплексом «Аккорд-АМДЗ» специальное ПО реализует дискреционный и мандатный (кроме версии 1.35) 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.

3. 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 (**ISA/PCI**) на материнской плате **ПЭВМ;**
- при поставке совместно с комплексом специального ПО – объем дискового пространства для его размещения на логическом диске **C:** для ПО **v.1.35** – около **1,2** Мбайт, для ПО **v.1.95** – около 3**,0** Мбайт, для ПО . **v. 2.0** – около **3,5** Мбайт.

При модификации внутреннего ПО замена контроллера не требуется. При этом обеспечивается поддержка спецрежима программирования контроллера 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, 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 ТМ-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**.

3. СОСТАВ КОМПЛЕКСА.

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

3.1. 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).

- ***Контактное устройство*** - съемник информации с ТМ- идентификаторов пользователей (устройств памяти DS 199x “Touch Memory.
- ***Персональные ТМ-идентификаторы пользователей–*** представляют собой полупассивные микропроцессорные устройства DS 199x ("Touch memory"), снабженные элементом питания, в виде "таблетки" диаметром **16 мм** и толщиной **3-5 мм** в удобной пластмассовой (металлической) оправке. Каждый ТМ-идентификатор обладает уникальным номером **(48 бит),** который формируется технологически и подделать который практически невозможно.

Объем доступной для записи/ чтения памяти составляет до **64 Кбит** в зависимости от типа идентификатора. Срок хранения записанной информации, обеспечиваемый элементом питания - не менее **10** лет.

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

3.2. 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

3.3. Специальное ПО СЗИ НСД.

По отдельному заказу, совместно с комплексом АМДЗ могут поставляться следующие версии ПО разграничения доступа:

v.1.35 – при работе ПЭВМ (PC) под управлением ОС MS DOS;
v.1.95 – при работе ПЭВМ (PC) под управлением ОС MS DOS, Windows 9x;
v.1.95_00 – при работе ПЭВМ (PC) под управлением ОС Windows 9x (с графическим интерфейсом);
v.2.0 – при работе ПЭВМ (PC) под управлением ОС Windows NT 4.0 (SP4-6)/2000/XP.

4. ЗАЩИТНЫЕ ФУНКЦИИ КОМПЛЕКСА.

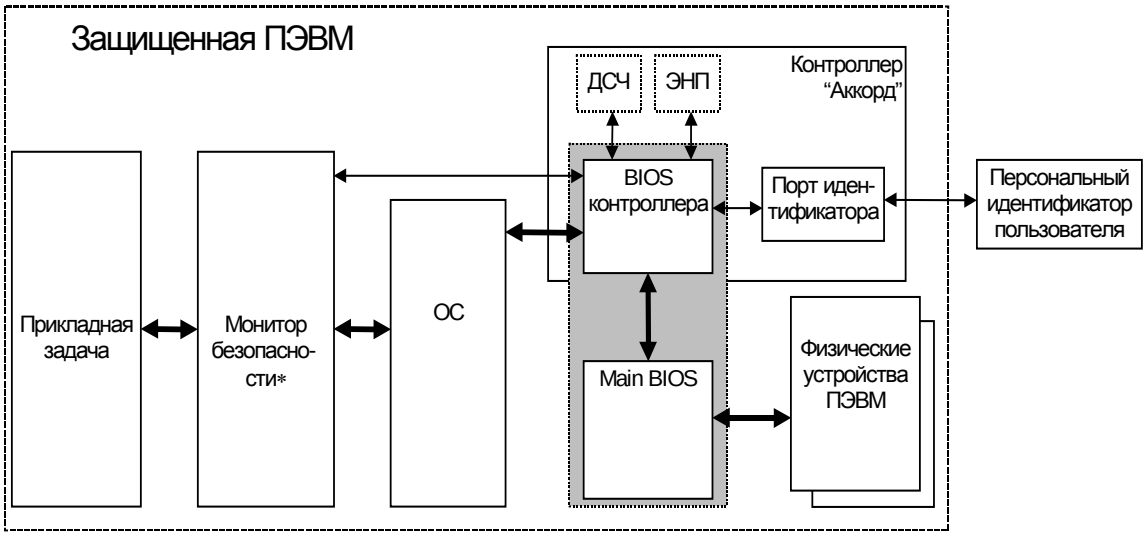
1.Защита от НСД к ПЭВМ, включая идентификацию пользователей по уникальному ТМ-идентификатору и их аутентификацию (подтверждение подлинности) с учетом необходимой длины пароля, времени его жизни, ограничением времени доступа субъекта к ПЭВМ (РС).

2. Контроль целостности критичных с точки зрения информационной безопасности системных областей и файлов, программ и данных до загрузки ОС- защита от несанкционированных модификаций и доверенной загрузки ОС.

3. Разграничение доступа к ресурсам ПЭВМ(АС) – реализуемой атрибутами доступа, которые устанавливаются администратором БИ каждой паре "Субъект доступа - объект доступа" при регистрации пользователей. Данная функция реализуется при установке специального ПО разграничения доступа на диск ПЭВМ.

4. Другие механизмы защиты в соответствии с нормативными документами.

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



Замечание к рисунку:Показанная система защиты с установленным специальном ПО

Рис.1.

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

1. На ПЭВМ 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 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 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-drave) для пользователей, не входящих в группу администраторов.

При касании съемника информации персональным идентификатором пользователя осуществляется поиск предъявленного идентификатора в списке зарегистрированных ТМ, который хранится в ЭНП контроллера. Если предъявленный идентификатор обнаружен в списке, то производится аутентификация пользователя и контроль целостности установленных в ПЭВМ 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 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.

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.

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

5. ФОРМИРОВАНИЕ И ПОДДЕРЖКА ИЗОЛИРОВАННОЙ ПРОГРАММНОЙ СРЕДЫ.

Предположим, что на ПЭВМ 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 программ либо субъектом, не входящим в *N* допущенных, либо i-м пользователем вне подмножества своих полномочий *Ti*. НСД осуществляется обязательно при помощи имеющихся на ПЭВМ или доставленных злоумышленником программных средств (в данном случае не рассматривается возможность нарушения целостности аппаратных средств ПЭВМ.

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 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 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, отсутствуют специально интегрированные в них возможности НСД.

Пусть пользователь ПЭВМ работает с программой, в которой также исключено наличие каких-либо скрытых возможностей (на ПЭВМ 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 гарантировано невозможен, если выполняются следующие условия:

У1. На ПЭВМ 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.

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.

Литература:

[1] Управление защитой информации на базе СЗИ НСД «Аккорд» В.А. Конявский.

[2] Программно-аппаратный комплекс средств защиты информации от НСД для ЭВМ(РС)“Аккорд–АМДЗ” (версии 2.0, 3.0, 4.0)ОПИСАНИЕ ПРИМЕНЕНИЯ

[3] http://www.accord.ru