ОКБ АПР ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

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

Описание применения
11443195.4012.046 31

Листов 23

Москва

АННОТАЦИЯ

Настоящий документ является описанием применения программно-аппаратного комплекса средств защиты информации от несанкционированного доступа «ИНАФ» (далее по тексту – «ИНАФ», комплекс, ПАК «ИНАФ», ПАК СЗИ НСД), являющегося средством доверенной загрузки.

В документе приведены основные защитные функции, возможности комплекса, условия технического, технологического и организационного характера, входные и выходные данные, задача применения «ИНАФ» и методы ее решения.

Перед установкой и эксплуатацией комплекса «ИНАФ» необходимо внимательно ознакомиться с комплектом эксплуатационной документации, а также принять необходимые организационные меры защиты, указанные в настоящей 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 «ИНАФ», 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 – 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.

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

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

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
ПРД	Правила (политики) разграничения доступа
ПЭВМ	Персональная электронно-вычислительная машина
РС	Рабочая станция
СВТ	Средство вычислительной техники
СДЗ	Средство доверенной загрузки
СЗИ	Средство защиты информации
ТУ	Технические условия
ФПО	Функциональное программное обеспечение
ЭНП	Энергонезависимая память
BIOS	basic input/output system - «базовая система ввода-вывода»
MBR	master boot record - Главная загрузочная запись
RAM	Random access memory
USB	Universal serial bus

1. Назначение комплекса

ПАК СЗИ НСД «ИНАФ» представляет собой программно-техническое средство, которое реализует функции по предотвращению несанкционированного доступа к программным и (или) техническим ресурсам средства вычислительной техники на этапе его загрузки в соответствии с требованиями документов «Профиль защиты средства доверенной загрузки уровня платы расширения четвертого класса защиты. ИТ.СДЗ.ПР4.ПЗ» и «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «ИНАФ». Задание по безопасности» (11443195.4012.046 ЗБ).

ПАК СЗИ НСД «ИНАФ» предназначен для применения на IBM-совместимых ПК (автономных ПК, серверах и рабочих станциях локальной сети) и обеспечивает защиту устройств и информационных ресурсов от НСД, контроль целостности файлов и областей жестких дисков (в том числе и системных) при многопользовательском режиме эксплуатации.

ПАК СЗИ НСД «ИНАФ» обеспечивает нейтрализацию следующих основных угроз безопасности информации:

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

Комплекс начинает работу сразу после выполнения кода системного BIOS компьютера – до загрузки операционной системы, и позволяет обеспечить возможность доверенной загрузки[1] для ОС, поддерживающих файловые системы: FAT12, FAT16, FAT32, NTFS, HPFS, Ext2, Ext3, Ext4, ReiserFS, FreeBSD UFS/UFS2, Solaris UFS, QNX4, MINIX.

ПАК СЗИ НСД «ИНАФ» обеспечивает:

- идентификацию и аутентификацию пользователей при входе в систему по персональному идентификатору пользователя и по паролю временного действия длиной от 0 до 12 буквенно-цифровых символов, введенных с клавиатуры;
- идентификацию и аутентификацию пользователей при допуске к средствам настройки и администрирования ПАК «ИНАФ» по персональному идентификатору пользователя и по паролю 0 до 12 буквенно-цифровых символов, введенных с клавиатуры;
- аппаратный контроль целостности технических, программных средств, условно-постоянной информации ПЭВМ до загрузки ОС, с реализацией пошагового алгоритма контроля;
- возможность доверенной загрузки операционной системы, а также системного и прикладного ПО при одновременной установке на дисках или в логических разделах диска ПЭВМ нескольких ОС;
- многопользовательский режим эксплуатации ПЭВМ с возможностью регистрации (в энергонезависимой памяти) до 1024 пользователей на одной ПЭВМ;
- администрирование, включающее:
    - регистрацию пользователей и их идентификаторов, генерацию пароля пользователя и определение его параметров;
    - построение списков объектов для контроля целостности и указание режимов контроля;
    - работу с журналом регистрации системных событий и действий пользователей.
- возможность резервного копирования на отчуждаемый носитель и восстановления базы данных пользователей и списка контролируемых объектов;
- регистрацию и учет системных событий и действий пользователей в системном журнале, размещенном в энергонезависимой памяти аппаратной части комплекса.

Программно-информационная часть комплекса, включающая в себя прошивку контроллера, базу контроля, журнал регистрации событий и

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

средства администрирования, размещена в энергонезависимой памяти контроллера. Этим обеспечивается возможность проведения процедур контроля целостности технических и программных средств СВТ, администрирования и аудита средствами «ИНАФ» на аппаратном уровне до загрузки ОС.

Комплекс обеспечивает выполнение основных функций защиты от НСД как в составе локальной СВТ, так и на рабочих станциях ЛВС в составе комплексной системы защиты от НСД ЛВС, в том числе настройку, контроль функционирования и управление комплексом.

Поскольку контроллер «ИНАФ» реализован в форм-факторе USB-устройства, он не требует для своей установки наличия на СВТ свободного PCI-слота и может применяться в случаях, когда используются blade-серверы, в которых отсутствуют PCI-слоты, но имеются свободные внутренние или внешние USB-разъемы (подробнее о возможных способах установки контроллера в СВТ см. 6.4).

3. Состав комплекса «ИНАФ»

Комплекс «ИНАФ» выпускается в программно-аппаратном исполнении.

Состав комплекса «ИНАФ»:

- специализированный контроллер (далее по тексту – контроллер) в форм-факторе, обеспечивающем подключение к шине USB с предустановленной на этапе изготовления резидентной операционной средой (специализированное программное обеспечение, СПО), который не реализует функциональные требования безопасности комплекса и представляет собой среду функционирования для функционального программного обеспечения;
- функциональное программное обеспечение (далее по тексту – ФПО), которое является ядром защиты комплекса, реализует функциональные требования безопасности комплекса и исполняется в резидентной операционной среде, предустановленной на специализированный контроллер.

Резидентная операционная среда включает:

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

В состав ФПО комплекса входят следующие функциональные модули:

- 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 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 ПАК «ИНАФ».

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

4. Условия применения

Комплекс «ИНАФ»:

- может использоваться в составе СВТ (PC) с центральным процессором архитектуры x86 (IA-32) или x86-64 (AMD64), с объемом динамической оперативной памяти (RAM) не менее 128 Мб;
- требует для установки свободный USB-разъем на корпусе СВТ или штырьковый USB-разъем на материнской плате СВТ, соответствующий варианту исполнения специализированного контроллера «ИНАФ»;
- предполагает наличие на СВТ любой из ОС, использующей поддерживаемую комплексом файловую систему.

При эксплуатации ПАК «ИНАФ» на объектах информатизации необходимо обеспечить обязательное выполнение следующих условий:

- регламентация запрета использования ПАК «ИНАФ» для обработки информации, содержащей сведения, составляющие государственную тайну;
- наличие администратора безопасности, отвечающего за правильную эксплуатацию ПАК «ИНАФ», в том числе:
    - регулярное выполнение контроля целостности программной части изделия;
    - разработку организационно-распорядительных документов, определяющих порядок допуска пользователей к информационным ресурсам автоматизированной системы и назначения их полномочий;
    - периодическое регламентное тестирование функциональных возможностей и механизмов защиты изделия при изменении настроек ПАК «ИНАФ»;
    - предотвращение несанкционированного доступа к идентификаторам и паролям привилегированных пользователей (администратора безопасности);
    - обеспечение физической сохранности ПЭВМ с установленным ПАК «ИНАФ» и исключение возможности доступа к ней/ним посторонних лиц;
    - задание и отслеживание соответствия паролей учетных записей пользователей следующим требованиям сложности: длина пароля не менее восьми символов, алфавит пароля не менее 70 символов.
- для нейтрализации уязвимости в технологиях Intel Trusted Execution Technology (TXT) SINIT для Authenticated Code Module (ACM) (CVE-2013-5740) в BIOS компьютера, на котором планируется использовать ПАК «ИНАФ», рекомендуется отключить опцию Intel®TXT. Если для работы ПЭВМ необходима опция Intel®TXT, то необходимо обновить модуль аутентифицированного кода SINIT

ACM. Обновленные инструменты SINIT ACM можно загрузить с http://software.intel.com/en-us/articles/intel-trusted-execution-technology/. Intel;

- для нейтрализации уязвимости аутентифицированного кода Intel SINIT, который позволял локальным пользователям получать повышенные привилегии (уязвимость CVE-2009-4419) необходимо произвести обновление данного кода. Обновленный код можно загрузить на сайте разработчика security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00021&languageid=en-fr

5. Описание задачи

«ИНАФ» – это простой и эффективный комплекс программно-аппаратных 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.

Комплекс соответствует требованиям по 4 уровню контроля отсутствия недекларированных возможностей[1], по 4 классу защиты средства доверенной загрузки уровня платы расширения[2], требованиям Задания по безопасности 11443195.4012.046 ЗБ и требованиям Технических условий ТУ 4012-046-11443195-2015.

Обеспечивается возможность использования комплекса для защиты информации в АС до класса защищенности 1Г[3], включительно.

Обеспечивается возможность использования комплекса для реализации мер защиты информации в государственных информационных системах до 1 класса защищенности включительно[4].

Обеспечивается возможность использования комплекса для реализации мер по обеспечению безопасности персональных данных до 1 уровня защищенности включительно[5].

Задачей функционирования «ИНАФ» является защита информации от НСД посредством обеспечения возможности выполнения доверенной загрузки ОС с применением следующих механизмов:

- контроля целостности технических средств ПЭВМ;
- контроля целостности системных областей жесткого диска;
- контроля целостности программных средств;

[1] В соответствии с требованиями руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации Классификация по уровню контроля отсутствия недекларированных возможностей», утвержденного решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. № 114.

[2] В соответствии с методическим документом «Профиль защиты средства доверенной загрузки уровня платы расширения четвертого класса защиты. ИТ.СДЗ.ПР4.ПЗ», утвержденным ФСТЭК России от 30 декабря 2013 г.

[3] В соответствии с требованиями руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Классификация автоматизированных систем и требования по защите информации», утвержденного решением председателя Гостехкомиссии России от 30 марта 1992 года.

[4] В соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденными Приказом № 17 ФСТЭК России от 11 февраля 2013 г.

[5] В соответствии с «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденными Приказом № 21 ФСТЭК России от 18 февраля 2013 г.

- регистрации и учета системных событий (работы с журналом регистрации событий);
- администрирования «ИНАФ».

Контроль целостности аппаратуры ПЭВМ осуществляется на аппаратном уровне контроллером «ИНАФ» до загрузки ОС.

Контроль целостности системных областей жестких дисков, программных средств ПЭВМ осуществляется контроллером «ИНАФ» на аппаратном уровне до загрузки ОС в указанных выше файловых системах.

В процессе выполнения механизма проверяются хэш-функции контролируемых областей жесткого диска (загрузочный сектор, логические диски и т.д.). В случае совпадения значений с эталонными происходит дальнейший процесс загрузки, в противном случае загрузка приостанавливается.

Механизм регистрации и учета системных событий (работы с журналом регистрации событий) обеспечивает регистрацию и учет следующих системных событий и действий пользователя:

- начало сеанса пользователя;
- прохождение процедуры аутентификации пользователем;
- осуществление контроля целостности аппаратуры ПЭВМ;
- осуществление контроля целостности отдельных файлов и программ;
- осуществление контроля целостности системных областей жестких дисков (секторов);
- осуществление контроля системного реестра (для ОС семейства Microsoft Windows);
- создание журнала системных событий и действий пользователей;
- изменение полномочий пользователей.

Журнал регистрации событий для каждого события содержит следующую информацию:

- дата и точное время регистрации события;
- тип события;
- идентификатор субъекта;
- результат события (успешный или неуспешный).

Администрирование комплекса «ИНАФ» может проводить только пользователь, зарегистрированный в группе «Администраторы». Состояние настроек комплекса однозначно определяет режим функционирования комплекса.

6. Порядок применения

6.1. Общие сведения

Контроль целостности технических и программных средств СВТ (РС) выполняется контроллером комплекса до загрузки операционной системы, установленной в СВТ (РС).

Комплекс обеспечивает выполнение основных функций защиты от НСД как в составе локальной СВТ, так и на рабочих станциях ЛВС в составе комплексной системы защиты от НСД ЛВС, в том числе настройку, контроль функционирования и управление комплексом.

В зависимости от конструктивных возможностей СВТ (РС) возможна установка контроллера «ИНАФ» внутри корпуса СВТ (РС) в качестве штатного устройства с USB-разъемом или установка во внешние USB-разъемы. Для подключения по USB-интерфейсу используется тип «А» USB-разъема. Также возможен вариант подключения к штырьковому разъему непосредственно на материнской плате СВТ.

Комплекс «ИНАФ» предназначен для обеспечения возможности доверенной загрузки ОС.

6.2. Особенности применения

В СЗИ НСД «ИНАФ» доступна регистрация пользователей, среди которых:

- пользователь «Гл. Администратор» (как правило, администратор безопасности информации) – пользователь, которому полностью доступны все функции администрирования (создание и удаление групп пользователей, а также учетных записей администраторов и пользователей), функции подсистемы контроля целостности (контроль аппаратуры, дисков, файлов и ветвей реестра), функции подсистемы аудита (системный журнал контроллера) и функции резервного копирования. Учетная запись «Гл. Администратор» создается автоматически при первом запуске комплекса;
- пользователи группы «Администраторы». Администраторы имеют возможность (при наличии соответствующих полномочий) редактировать списки и настройки пользователей, осуществлять постановку ресурсов на контроль целостности и просматривать системный журнал контроллера;
- пользователи группы «Обычные». Пользователи имеют возможность работы на ПЭВМ после прохождения процедур идентификации и аутентификации, а также если объекты, поставленные на контроль целостности, прошли процедуру проверки.

При инициализации контроллера создаются две зарезервированные группы пользователей – «ADMINS» (далее – «Администраторы») и «EVERYONE» (далее– «Обычные»). Эти две группы нельзя ни

переименовать, ни удалить. Для каждой из групп можно задать общие параметры, которые будут устанавливаться по умолчанию при создании пользователя в группе. Для каждого зарегистрированного пользователя можно изменить данные параметры при индивидуальной настройке. Такие же правила будут выполняться и для любой группы, созданной администратором.

6.3. Порядок работы

Для работы с комплексом «ИНАФ» необходимо выполнить следующие действия:

- установить контроллер «ИНАФ» в соответствующий порт СВТ;
- установить пароль для входа в BIOS;
- после включения питания СВТ в BIOS необходимо выбрать вариант загрузки «ИНАФ» как с жесткого диска;
- после загрузки ОС комплекса с жесткого диска необходимо выполнить установку параметров учетной записи «Гл. Администратор»;
- по завершении процедуры установки параметров учетной записи «Гл. Администратор» выполняется вход в ОС Linux под учетной записью «Гл. Администратор», где доступны параметры конфигурации для подсистем контроля целостности и аудита;
- создать необходимое количество учетных записей администраторов и обычных пользователей, каждому из которых регистрируется идентификатор пользователя и назначается пароль. Для каждого пользователя комплекса настраиваются индивидуальные параметры пользователей (персональные параметры, параметры авторизации и т.п.);
- выбрать для каждого пользователя комплекса необходимые объекты для контроля целостности.

6.4. Сценарии применения

6.4.1. Общие сведения

Комплекс может использоваться в рамках реализации двух типов сценариев:

- стационарная установка в СВТ. В зависимости от конструктивных возможностей СВТ возможна как установка внутри корпуса в качестве штатного устройства с USB-разъемом типа «А», так и подключение к штырьковому разъему непосредственно на материнской плате;
- использование в качестве мобильного устройства с подключением контроллера «ИНАФ» во внешние USB-разъемы СВТ (PC).

6.4.2. Стационарная установка в СВТ

Данный тип сценария используется в том случае, когда необходима непрерывная реализация функционала «ИНАФ». В этом случае контроллер соответствующим образом настроен и подключен к USB-порту СВТ постоянно. Каждый раз перед загрузкой ОС пользователем СВТ контроллер «ИНАФ» выполняет процедуру контроля целостности определенных заранее объектов. В случае нарушения целостности загрузка ОС блокируется и требуется вмешательство администратора «ИНАФ» (пользователь из группы «Администраторы», обладающий соответствующими правами на администрирование комплекса).

Для корректной работы по данному типу сценария необходимо:

1. установить в BIOS вариант загрузки с «ИНАФ» как с жесткого диска;
2. установить пароль на вход в BIOS;
3. принять административные меры, исключающие несанкционированное отключение устройства от USB-порта:
   - ограничить физический доступ к СВТ и/или
   - зафиксировать устройство с помощью специальных креплений и/или голографической наклейки или установить контроллер внутрь корпуса СВТ.

6.4.3. Использование в качестве мобильного устройства

Данный тип сценария используется в том случае, когда нет необходимости выполнять процедуры контроля целостности объектов постоянно и запрещать для пользователей СВТ загрузку ОС в случае нарушения целостности, а нужно только выявить сам факт нарушения целостности установленных на контроль объектов.

В этом случае сначала выполняются все необходимые настройки подключенного к СВТ контроллера «ИНАФ», затем контроллер извлекается из СВТ и хранится в надежном месте (например, в сейфе). Пользователи СВТ работают в обычном режиме, а обладающий соответствующими правами пользователь «ИНАФ» периодически подключает к СВТ свой контроллер «ИНАФ» с целью убедиться в неизменности состава СВТ и установленных ранее на контроль объектов.

Возможен также вариант работы с «ИНАФ», когда контроллер подключается к СВТ каждый раз перед началом сеанса работы и извлекается из СВТ после ее выключения.

Для корректного осуществления работы по данному типу сценария обязательно должны быть предусмотрены специальные регламенты действий пользователей ПЭВМ, в чьи обязанности входит запуск ПЭВМ, так как наличие «ИНАФ» в USB-порту должны контролировать именно они.

Следует помнить о том, что поскольку для работы с «ИНАФ» требуется настраивать порядок загрузки ОС в BIOS компьютера, необходимо накладывать определенные ограничения (особенно в случае стационарной установки «ИНАФ» в СВТ) на доступ пользователей СВТ к BIOS (путем установки пароля на BIOS), а также контролировать целостность BIOS средствами «ИНАФ».

7. Входные и выходные данные

7.1. Входные данные

Входными данными для «ИНАФ» являются:

- идентификатор пользователя;
- пароль для входа в «ИНАФ»;
- параметры подсистемы контроля целостности комплекса, реализующие защитные функции:
    - контроля целостности программных средств;
    - контроля целостности отдельных ветвей реестра (для ОС семейства Windows);
    - контроля целостности системных областей жесткого диска;
    - контроля целостности технических средств ПЭВМ (PC).
- параметры настройки подсистемы аудита (работа с журналом регистрации событий);
- параметры подсистемы администрирования;

7.1.1. Идентификатор пользователя

Идентификатор пользователя представляет собой устройство, на котором записана информация, идентифицирующая пользователя при входе в систему.

Комплекс поддерживает работу с персональными идентификаторами, список которых приведен в таблице 1.

Таблица 1 - Персональные идентификаторов пользователя, поддерживаемые комплексом «ИНАФ»

Наименование и обозначение	Производитель (страна, фирма)	Характеристика
JaCarta PKI[1]	Россия, ЗАО «Аладдин Р.Д.»	Защищённый смарт-карточный чип, имеющий специальную сертифицированную защиту и на аппаратном, и на программном уровнях

7.1.2. Пароль

Пароль — условное слово или набор знаков, предназначенный для подтверждения личности при входе в систему.

В «ИНАФ» используется пароль длиной до 12 символов. Комплекс поддерживает возможность генерации случайного пароля требуемой длины.

Для проведения процедуры аутентификации предусмотрен режим отображения пароля в скрытом виде при вводе - в виде символов <*>. Этим

[1] Сертификат соответствия № 2799, выданный ФСТЭК России 28 декабря 2012г, действителен до 28 декабря 2015г, продлен до 28 декабря 2018г.

затрудняется возможность раскрытия личного пароля и использования утраченного (похищенного) идентификатора.

7.1.3. Параметры подсистемы контроля целостности

Входные данные подсистемы контроля целостности представляют собой поля в интерфейсе «ИНАФ», при заполнении которых задаются объекты для контроля целостности. Такими данными являются поля, содержащие информацию:

- о программных средствах;
- об отдельных ветвях реестра (для ОС семейства Windows);
- о системных областях жесткого диска;
- о технических средствах ПЭВМ (PC);

7.1.4. Параметры подсистемы аудита

Входные данные подсистемы аудита работы системы – поля в интерфейсе «ИНАФ», редактирование которых позволяет составлять необходимую конфигурацию журнала регистрации событий.

7.1.5. Параметры подсистемы администрирования комплекса

Входные данные подсистемы администрирования представляют собой поля с информацией о настройках учетных записей всех зарегистрированных в комплексе пользователей.

7.2. Выходные данные

Выходными данными для «ИНАФ» являются:

- готовые списки программ, файлов, технических средств ПЭВМ, системных областей жесткого диска и ветвей реестров, по результатам анализа которых выносится решение о прохождении процедуры контроля целостности;
- результат, выносимый подсистемой идентификации и аутентификации пользователей;
- файлы логов, формирующиеся по результатам работы подсистемы аудита;
- списки пользователей комплекса «ИНАФ» с определенными для них параметрами учетных записей, сформированные в результате работы подсистемы администрирования.

8. 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 Ta,
- 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.

Приложение 2.
Методика определения требуемой (целесообразной) длины пароля, используемого в СЗИ НСД «ИНАФ» 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 «ИНАФ»– 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***.