ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
ОКБ
систем автоматизированного проектирования

УТВЕРЖДЕН
37222406.26.20.40.140.080 31-ЛУ

Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа

«АККОРД-Х»

ОПИСАНИЕ ПРИМЕНЕНИЯ

37222406.26.20.40.140.080 31

АННОТАЦИЯ

Настоящий документ является описанием применения специального программного обеспечения программно-аппаратного комплекса средств защиты информации от несанкционированного доступа «Аккорд-X» и предназначен для лиц, планирующих и организующих защиту информации в автоматизированных системах на базе СВТ (автономных ПК, рабочих станциях ЛВС, терминальных серверах), функционирующих под управлением ОС семейства Linux.

В документе приведены нормативные требования по защите информации, общие принципы и правила организации работы по обеспечению конфиденциальности информации, основные защитные функции ПАК СЗИ НСД «Аккорд-X», его возможности, особенности установки и применения.

Перед установкой и эксплуатацией ПАК СЗИ НСД «Аккорд-X» необходимо внимательно ознакомиться с комплектом эксплуатационной документации, а также принять необходимые организационные меры защиты.

Применение защитных механизмов ПАК СЗИ НСД «Аккорд-X» должно дополняться общими мерами предосторожности и физической безопасности СВТ.

СОДЕРЖАНИЕ

1 НОРМАТИВНЫЕ ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

1.1 Необходимость и цели защиты информации

Развитие средств вычислительной техники, автоматизированных информационных систем, появление новых информационных технологий сопровождается, к сожалению, и появлением таких малоприятных явлений, как промышленный шпионаж, компьютерная преступность и, прежде всего, несанкционированный доступ (НСД) к конфиденциальной информации. Этим обуславливается актуальность и значимость проблемы защиты информации.

Острая необходимость в защите информации нашла выражение в создании Государственной системы защиты информации (ГСЗИ). Развивается правовая база информационной безопасности. Приняты и введены в действие законы «О государственной тайне», «Об информации, информатизации и защите информации», «О правовой охране программ для электронных вычислительных машин и баз данных» и др.

Целями защиты информации являются:

- предотвращение ущерба, возникновение которого возможно в результате утери (хищения, утраты, искажения, подделки) информации в любом ее проявлении;
- реализация мер защиты, адекватных угрозам безопасности информации, в соответствии с действующими Законами и нормативными документами по безопасности информации;
- реализация мер защиты, в соответствии с потребностями владельцев (пользователей) информации.

Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.[1]

Любое современное предприятие (учреждение, фирма и т.д.), независимо от вида деятельности и форм собственности, не может сегодня успешно развиваться и вести хозяйственную и иную деятельность без создания надежной системы защиты своей информации.

Система защиты информации должна включать в себя не только организационно-нормативные меры, но и технические средства контроля безопасности информации при ее обработке, хранении и передаче в автоматизированных системах (АС), прежде всего, программно-аппаратные.

1.2 Основные принципы организации защиты информации от НСД

Мероприятия по защите информации от НСД являются составной частью управленческой, научной, производственной (коммерческой)

[1] *Закон Российской Федерации «Об информации, информатизации и защите информации»*

деятельности предприятия (учреждения, фирмы и т.д.), независимо от их ведомственной принадлежности и формы собственности, и осуществляются в комплексе с другими мерами по обеспечению установленного режима конфиденциальности. Практика организации защиты информации от НСД при ее обработке и хранении в автоматизированных системах (АС) должна учитывать следующие принципы и правила обеспечения безопасности информации:[2]

соответствие уровня безопасности информации законодательным положениям и нормативным требованиям по охране сведений, подлежащих защите по действующему законодательству, в т.ч. выбор класса защищенности АС в соответствии с особенностями обработки информации (технология обработки, конкретные условия эксплуатации АС) и уровнем ее конфиденциальности;

выявление конфиденциальной информации и документальное оформление в виде перечня сведений, подлежащих защите, его своевременная корректировка;

наиболее важные решения по защите информации должны приниматься руководством предприятия (организации, фирмы), владельцем АС;

определение уровней полномочий субъектов доступа, а также круга лиц, которым предоставлено право присвоения уровней полномочий;

установление и оформление правил разграничения доступа (ПРД), т.е. совокупности правил, регламентирующих права доступа субъектов доступа к объектам доступа;

установление личной ответственности пользователей за поддержание уровня защищенности АС при обработке сведений, подлежащих защите по действующему законодательству путем:

- ознакомления с перечнем защищаемых сведений, организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации;
- определения уровня полномочий в соответствии с его должностными обязанностями;
- получения от субъекта доступа расписки о неразглашении доверенной ему конфиденциальной информации;

обеспечение физической охраны объекта, на котором расположена защищаемая АС (территория, здание, помещение, хранилище информационных носителей) путем установления соответствующих постов, технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими хищение средств вычислительной техники (СВТ), информационных носителей, а также НСД к СВТ и линиям связи;

---

[2] *РД. АС. Защита от НСД к информации. Классификация АС и требования по защите информации. -М.: Гостехкомиссия России, 1992.*

организация службы безопасности информации (ответственные лица, администраторы), осуществляющей учет, хранение и выдачу информационных носителей, паролей, ключей, ведение служебной информации (генерация паролей, ключей, сопровождение правил разграничения доступа), приемку включаемых в АС новых программных средств, а также контроль за ходом технологического процесса обработки конфиденциальной информации и т.д.;

планомерный и оперативный контроль уровня безопасности защищаемой информации, в т.ч. проверка защитных функций средств защиты информации.

Средства защиты информации должны иметь СЕРТИФИКАТ, удостоверяющий их соответствие требованиям по безопасности информации в соответствии с действующими Законами и нормативными документами по безопасности информации.

2 ОБЩИЕ СВЕДЕНИЯ

ПАК СЗИ НСД «Аккорд-X» (далее - ПАК «Аккорд-X», «Аккорд-X», комплекс «Аккорд-X», Комплекс) представляет собой комплекс программных и аппаратных средств, который предназначен для применения в СВТ типа IBM PC (автономных ПК, рабочих станциях ЛВС, терминальных серверах), функционирующих под управлением ОС семейства Linux (список поддерживаемых ОС см. в Формуляре на комплекс «Аккорд-X» (37222406.26.20.40.140.080 ФО)) с целью обеспечения защиты от несанкционированного доступа к информации при многопользовательском режиме эксплуатации.

Комплекс включает в себя:

- аппаратную часть: контроллер «Аккорд-АМДЗ» (ТУ 4012-038-11443195-2011, ТУ 26.20.40.140-079-37222406-2019, ТУ 4012-054-11443195-2013), съемник информации с контактным устройством, персональный идентификатор пользователя;
- специальное программное обеспечение «Аккорд-X».

В составе СЗИ НСД «Аккорд-АМДЗ» могут применяться специализированные контроллеры, имеющие шинный интерфейс PCI (5 В), PCI-X (3,3 В), PCI-Express (PCI-E), miniPCI, miniPCI-E, M.2.

Состав Комплекса (тип контроллера и съемника информации с контактным устройством, тип и количество идентификаторов) определяется при заказе Комплекса в соответствии с требованиями Заказчика и указывается в документе «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-X». Формуляр» (37222406.26.20.40.140.080 ФО).

СПО «Аккорд-X» выполняет следующие функции:

- разграничение доступа пользователей к локальным и сетевым ресурсам ПЭВМ (АС), в том числе к внешним устройствам, в соответствии с принципами дискреционного доступа и доступа на основе иерархических меток, а также управление потоками информации, что исключает возможность несанкционированного переноса информации из объектов с меньшим уровнем доступа конфиденциальности в объекты с большим уровнем конфиденциальности;
- реализация дискреционного механизма и механизма разграничения доступа на основе иерархических меток и обеспечения управления потоками информации, исключая возможность ее несанкционированного переноса из объектов с меньшим уровнем конфиденциальности в объекты с большим уровнем;
- создание изолированной программной среды, исключающей внедрение в систему вредоносных или неразрешенных Администратором БИ программ;
- очистки памяти на внешних носителях;

- контроль печати, который позволяет контролировать процессы, документы, принтеры и автоматически маркировать распечатываемые листы специальными пометками, грифами и т.д.;
- идентификация и аутентификация пользователей по уникальному идентификатору;
- аутентификация с учетом необходимой длины пароля;
- контроль целостности программ и данных по спискам контроля целостности (статический и динамический контроль целостности);
- управление процедурами ввода/вывода на отчуждаемые носители информации;
- регистрация контролируемых событий в системном журнале, доступ к которому предоставляется только Администратору БИ.

3 ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ И ОРГАНИЗАЦИОННЫЕ МЕРЫ, НЕОБХОДИМЫЕ ДЛЯ ПРИМЕНЕНИЯ КОМПЛЕКСА

3.1 Технические требования

Для установки Комплекса требуется следующий минимальный состав технических и программных средств:

- IBM PC AT, совместимая с процессором и объемом RAM, обеспечивающим применение операционных систем семейства Linux (список поддерживаемых ОС см. в Формуляре на комплекс «Аккорд-X» (37222406.26.20.40.140.080 ФО));
- наличие на СВТ (РС) HDD и CD ROM для установки Специального программного обеспечения «Аккорд-X» (далее по тексту – СПО);
- объем дискового пространства для установки СПО – не менее 128 Мб;
- наличие свободного слота на материнской плате СВТ (РС), соответствующего типу используемого контроллера, для установки специализированного контроллера.

В Н И М А Н И Е !

До начала установки комплекса «Аккорд-X» необходимо убедиться, что система входит в список поддерживаемых ОС.

При применении Комплекса следует помнить, что количество пользователей, регистрируемых на одной СВТ (РС), ограничено объемом энергонезависимой памяти контроллеров «Аккорд-АМДЗ» (подробнее см. документацию на «Аккорд-АМДЗ»).

Аппаратные средства, используемые в составе Комплекса, проверены на совместимость практически со всем доступным разработчику программно-аппаратным обеспечением СВТ (РС) как зарубежного, так и отечественного производства. Совместимость обеспечивается правильной установкой и настройкой Комплекса.

3.2 Организационные меры

Для эффективного применения Комплекса и поддержания необходимого уровня защищенности СВТ (РС) и информационных ресурсов АС **необходимо**[3]:

- наличие администратора безопасности информации (супервизора; далее по тексту – Администратор БИ) – привилегированного пользователя, имеющего особый статус и абсолютные полномочия.

---

[3] более подробно приведены в документах «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-X». Руководство администратора» и «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-X». Руководство оператора (пользователя)»

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. Более подробно обязанности Администратора БИ по применению Комплекса изложены в «Руководстве администратора» (37222406.26.20.40.140.080 90);

- физическая охрана СВТ (АС) и ее средств, в том числе проведение мероприятий по недопущению изъятия контроллера Комплекса;
- использование в СВТ (АС) технических и программных средств, сертифицированных как в Системе ГОСТ Р, так и в Государственной системе защиты информации.

4 ОСОБЕННОСТИ ЗАЩИТНЫХ ФУНКЦИЙ КОМПЛЕКСА

ПАК «Аккорд-Х» обеспечивает выполнение «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2018) и функциональных требований технических условий (ТУ 26.20.40.140-080-37222406-2019).

Комплекс соответствует требованиям по 2 уровню доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий.

В Комплексе обеспечена возможность использования для защиты информации в АС до класса защищенности 1Б.

В Комплексе обеспечена возможность использования для реализации мер защиты информации в государственных информационных системах до 1 класса защищенности включительно.

В Комплексе обеспечена возможность использования для реализации мер по обеспечению безопасности персональных данных до 1 уровня защищенности включительно.

В Комплексе реализована возможность обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации до 1 категории значимости включительно.

В Комплексе обеспечена защита информации, обработка которой осуществляется автоматизированными системами управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды до 1 класса защищенности.

Защитные функции Комплекса реализуются применением:

1. Дисциплины защиты от НСД СВТ (РС), включая:
   - идентификацию пользователя по уникальному идентификатору (список поддерживаемых идентификаторов приведен в Конфигураторе К 37222406.26.20.40.140.080);
   - аутентификацию с учетом необходимой длины пароля;
   - аппаратный (до загрузки операционной системы) контроль целостности технических средств СВТ (РС), программ и данных на жестком диске (в том числе системных областей диска);
   - ограничение времени доступа субъекта к СВТ (АС) в соответствии с установленным режимом работы пользователей;
   - блокировку несанкционированной загрузки СВТ (РС) с отчуждаемых носителей (FDD, CD-ROM, ZIP-drive).
2. Дисциплины разграничения доступа к ресурсам СВТ (АС) в соответствии с установленными ПРД и определяемыми атрибутами доступа, которые устанавливаются администратором безопасности информации (Администратором БИ) соответственно каждой паре «субъект доступа - объект доступа» при регистрации пользователей.

Комплекс позволяет Администратору БИ использовать как дискреционный метод, так и метод разграничения доступа на основе иерархических меток, и обеспечивает управление потоками информации, исключая возможность ее несанкционированного переноса из объектов с меньшим уровнем конфиденциальности в объекты с большим уровнем;

3. Дисциплины управления процедурами ввода/вывода на отчуждаемые носители информации. Подсистема контроля вывода на печать осуществляет маркировку печатных документов и запрещает вывод на незарегистрированные печатающие устройства;
4. Контроля целостности критичных с точки зрения информационной безопасности программ и данных (дисциплины защиты от несанкционированных модификаций). Кроме процедур, выполняемых контроллером Комплекса, в программной части Комплекса возможна проверка целостности программ и данных по индивидуальному списку для отдельного пользователя или группы пользователей. Подсистема контроля целостности предусматривает как статический список (проверка выполняется однократно в начале сеанса), так и динамический список, проверка по которому выполняется перед каждой загрузкой контролируемого файла в оперативную память;
5. Средств создания изолированной программной среды, исключающей внедрение в систему вредоносных или неразрешенных Администратором БИ программ (методические рекомендации по формированию и поддержке изолированной программной среды приведены в Приложении А);
6. Механизма очистки оперативной памяти и памяти на внешних носителях;
7. Регистрации действий пользователей в системном журнале, доступ к которому предоставляется только Администратору БИ;
8. Ввода широкого перечня дополнительных защитных механизмов в соответствии с политикой информационной безопасности, принятой в организации (на предприятии, фирме и т.д.).

Комплекс может применяться в произвольной и функционально замкнутой программной среде, обеспечивая при этом:

- защиту от несанкционированного доступа к СВТ (АС) и их ресурсам;
- разграничение доступа к ресурсам СВТ (АС), в т.ч. к внешним устройствам, в соответствии с уровнем полномочий пользователей;
- защиту от несанкционированных модификаций программ и данных, внедрения разрушающих программных воздействий (РПВ);
- защиту от несанкционированного изменения конфигурации технических и программных средств СВТ (РС);
- функциональное замыкание информационных систем с исключением возможности несанкционированного входа в операционную систему и загрузки с внешнего носителя;

- регистрацию действий пользователей в системном журнале, доступ к которому предоставляется только Администратору БИ.

В Комплексе используются и некоторые дополнительные механизмы защиты от НСД к СВТ (АС). Так, в частности, для пользователя Администратор БИ может установить:

- минимальную длину пароля (см. Приложение Б);
- временные ограничения использования СВТ для пользователей путем определения и установки интервала времени по дням недели (с дискретностью 30 мин), в котором разрешена работа для данного пользователя;
- подачу соответствующих звуковых и визуальных сигналов при попытках несанкционированного доступа к СВТ (в АС) и к их ресурсам.

5 ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ КОМПЛЕКСА

Схема построения системы защиты информации с использованием Комплекса и ее взаимодействие с программно-аппаратным обеспечением СВТ показаны на рисунке 1.

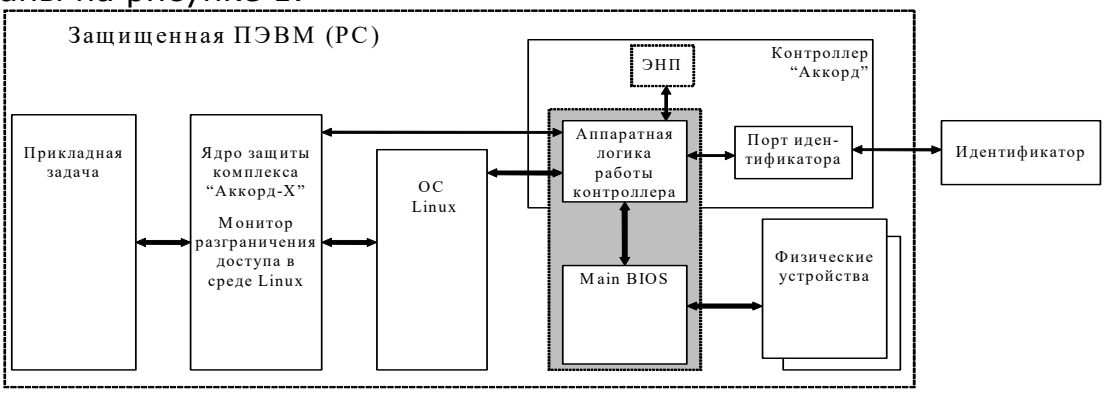

Рисунок 1. Схема построения системы защиты информации

Защита информации с использованием средств Комплекса основана на обработке событий, возникающих при обращении прикладных программ или системного программного обеспечения к ресурсам СВТ. Средства Комплекса перехватывают соответствующие программные и/или аппаратные прерывания, анализируют запрос и в зависимости от соответствия полномочий субъекта доступа (или его прикладной задачи) либо разрешают операционной системе обработку этих событий, либо запрещают (передают операционной системе код ошибки).

Комплекс состоит из собственно средств защиты СВТ от НСД и средств разграничения доступа к его ресурсам, которые условно можно представить в виде взаимодействующих между собой подсистем защиты информации (рисунок 2).

Рисунок 2. Укрупненная схема Комплекса

5.1 Подсистема управления доступом

Подсистема управления доступом включает в себя подсистему идентификации/аутентификации, предназначенную для защиты СВТ от посторонних[4] пользователей, и подсистему разграничения доступа – для управления доступом к объектам доступа и организации их совместного использования зарегистрированными пользователями в соответствии с установленными правилами разграничения доступа (ПРД).

Защита от посторонних пользователей обеспечивается процедурами идентификации (сравнение предъявленного идентификатора с перечнем зарегистрированных на СВТ) и аутентификации (подтверждение подлинности) с защитой от раскрытия пароля. Для идентификации пользователей используются персональные идентификаторы.

В Комплексе реализованы принципы дискреционного управления доступом и управления на основе иерархических меток.

При использовании дискреционного управления доступом зарегистрированному пользователю устанавливаются права доступа по принципу регистрации «белого списка» разрешенных к запуску программ (задач) и данных, а также «черного списка» запрещенных ресурсов, которые прописываются в ПРД.

При использовании ~~мандатного~~ управления доступом на основе иерархических меток пользователю (субъекту) устанавливается уровень доступа, а объекту (файлу, папке, сетевому ресурсу, съемному диску) присваивается метка доступа (гриф). При запросе пользователя на доступ к объекту, в зависимости от уровня полномочий пользователя, разрешается или запрещается запрошенный тип доступа.

Возможно использование одновременно двух механизмов доступа.

Настройка подсистемы разграничения доступом Комплекса осуществляется Администратором БИ с использованием утилиты acx-admin (см. документ «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-X». Руководство администратора» (37222406.26.20.40.140.080 90), входящий в состав эксплуатационной документации на Комплекс).

5.2 Подсистема регистрации и учета

Подсистема регистрации и учета предназначена для регистрации в системном журнале событий, обрабатываемых ПАК СЗИ НСД «Аккорд-АМДЗ» и подсистемой разграничения доступа «Аккорд-X».

При регистрации событий в системном журнале указываются:

- дата и время события;
- пользователь, осуществляющий регистрируемое действие;
- действия пользователя (сведения о входе/выходе пользователя в/из системы, запуске программ, фактах НСД и другие события).

[4] *Под посторонними пользователями понимаются все лица, не зарегистрированные в системе (не имеющие зарегистрированного в конкретном СВТ (РС) идентификатора).*

Перечень регистрируемых событий, их описание приводится в документе «ПАК СЗИ НСД «Аккорд-X». Руководство администратора» (37222406.26.20.40.140.080 90).

Работа с системными журналами осуществляется с использованием утилиты acx-admin log (см. документ «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-X». Руководство администратора» (37222406.26.20.40.140.080 90), входящий в состав эксплуатационной документации на Комплекс).

В Н И М А Н И Е !
Доступ к системному журналу возможен только Администратору БИ

5.3 Подсистема обеспечения целостности

Подсистема обеспечения целостности предназначена для исключения несанкционированных модификаций (как случайных, так и злоумышленных) конфигурации технических средств СВТ, программной среды, обрабатываемой информации, обеспечивая при этом защиту СВТ от внедрения программных закладок и вирусов.

Контроль целостности в Комплексе реализуется путем:

- проверки целостности конфигурации технических средств СВТ перед каждым сеансом работы пользователя;
- проверки целостности назначенных для контроля системных файлов, пользовательских программ и данных;
- исключением возможности использования СВТ без контроллера Комплекса;
- создания замкнутой программной среды, запрещающей запуск измененных программ.

Функционирование подсистемы обеспечения целостности в Комплексе основано на использовании следующих механизмов:

- при проверке на целостность вычисляется контрольная сумма файлов и сравнивается с эталонным (контрольным) значением, хранящимся в базе данных пользователей. Эти данные заносятся в энергонезависимую память контроллера Комплекса при регистрации пользователя и могут изменяться в процессе эксплуатации СВТ;
- для исключения фактов необнаружения модификации файла используется алгоритм расчета контрольных сумм - вычисление значения их хэш-функций (см. Приложение В). Эталонное (контрольное) значение хэш-функции контрольной суммы хранится вне СВТ (при контроле целостности средствами Аккорд-АМДЗ) - в энергонезависимой памяти контроллера, и этим защищается от несанкционированной модификации;
- защита от модификации программы расчета хэш-функций обеспечивается тем, что она хранится в памяти контроллера Комплекса;
- при контроле целостности индивидуального списка файлов пользователя результирующая хэш-функция хранится на жестком

диске, но в алгоритме расчета используется секретный ключ пользователя, записанный в идентификаторе;

- секретный ключ пользователя формируется из последовательности случайных чисел и записывается в идентификатор пользователя при регистрации. Этот секретный ключ используется при выработке КС и исключает возможность несанкционированной модификации файлов из индивидуального списка контролируемых файлов.

6 СОСТАВ КОМПЛЕКСА

6.1 Аппаратные средства

Аппаратные средства ПАК «Аккорд-Х» включают в себя:

контроллер АМДЗ, входящий в состав ПАК СЗИ НСД «Аккорд-АМДЗ» (ТУ 4012-038-11443195-2011, ТУ 26.20.40.140-079-37222406-2019, ТУ 4012-054-11443195-2013) - представляет собой карту расширения (expansion card), устанавливаемую в свободный слот материнской платы СВТ (РС). Контроллер является универсальным, не требует замены при изменении используемого типа операционной системы (ОС). В составе СЗИ НСД «Аккорд-АМДЗ» могут применяться специализированные контроллеры, имеющие шинный интерфейс PCI (5 В), PCI-X (3,3 В), PCI-Express (PCI-E), miniPCI, miniPCI-E, M.2;

съемник информации с контактным устройством, обеспечивающий интерфейс между контроллером Комплекса и персональным идентификатором пользователя. Съемник информации может быть:

- внешним - соединительный провод находится вне корпуса СВТ (РС) и подключение осуществляется к задней планке контроллера (или к соответствующим портам СВТ);
- внутренним - соединительный провод находится внутри корпуса СВТ (РС), подключение осуществляется с помощью разъема, находящегося на плате контроллера.

Контактное устройство внешних съемников крепится в удобном для пользователя месте (на корпусе СВТ (РС), мониторе, рабочем столе и т.д.) при помощи клейкой основы. Крепление контактного устройства внутреннего съемника осуществляется обычно в отверстии, высверливаемом на резервной заглушке дисковода передней панели СВТ (РС), с помощью гайки либо пружинной или резиновой шайбы;

персональный идентификатор пользователя – микропроцессорное устройство DS 199x («Touch memory»), ПАК «Персональный идентификатор ШИПКА», Рутокен Lite, Рутокен эцп 2.0, Рутокен 2151, JaCarta, ESMART Token. Каждый идентификатор обладает уникальным номером, который формируется технологически. Объем памяти, доступной для записи и чтения, зависит от типа идентификатора.

Количество и тип идентификаторов, модификация контроллера и контактного устройства оговариваются при поставке комплекса и указываются в документе «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «АККОРД-Х». Формуляр» (37222406.26.20.40.140.080 ФО).

6.2 Программные средства

Специальное программное обеспечение «Аккорд-Х» включает в себя:

ядро защиты – программы, реализующие защитные функции Комплекса;

программы управления защитными функциями Комплекса (настройки Комплекса в соответствии с ПРД).

7 ПРИНЦИП РАБОТЫ КОМПЛЕКСА

Плата контроллера Комплекса устанавливается в свободный слот материнской платы СВТ (РС). После установки платы Администратор БИ должен корректным образом настроить СЗИ НСД «Аккорд-АМДЗ» для выполнения контрольных процедур до загрузки ОС (см. «Руководство администратора» на комплекс Аккорд-АМДЗ).

После корректной настройки СЗИ НСД «Аккорд-АМДЗ» Администратор БИ должен корректным образом настроить программную часть комплекса «Аккорд-Х» (см. «Руководство администратора» на комплекс Аккорд-Х (37222406.26.20.40.140.080 90)). Активизация монитора разграничения доступа, настройка Комплекса, регистрация пользователей и установка правил разграничения доступа выполняются только Администратором БИ.

При регистрации пользователей Администратором БИ определяются их права доступа: список исполняемых программ и модулей, разрешенных к запуску данным пользователем, и список прав доступа к объектам (ресурсам) с использованием дискреционного механизма и/или механизма разграничения на основе иерархических меток (см. документ «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-Х». Руководство администратора» (37222406.26.20.40.140.080 90)).

С помощью утилиты acx-admin в специальный файл данных вносятся списки файлов, целостность которых будет проверяться при запуске СВТ (РС) данным пользователем. После регистрации пользователю выдается персональный идентификатор, о чем делается запись в журнале учета носителей информации.

Особенностью и, несомненно, преимуществом комплекса «Аккорд-Х» является проведение процедур идентификации, аутентификации и контроля целостности (аппаратуры, файлов, системных областей диска) до загрузки операционной системы. Это обеспечивается при помощи микропроцессора и энергонезависимой памяти, установленных на плате контроллера «Аккорд-АМДЗ». Внутреннее программное обеспечение контроллера, которое выполняет эти процедуры, защищено от модификации со стороны любого программного обеспечения, установленного на СВТ, т.к. хранится в области памяти, защищенной от записи.

Контроллер «Аккорд-АМДЗ» из состава комплекса СЗИ НСД «Аккорд - Х» получает управление в период выполнения так называемой процедуры ROM-SCAN. Суть данной процедуры заключается в следующем - в процессе начального старта, после проверки основного оборудования, BIOS компьютера начинает поиск внешних ПЗУ в диапазоне от C800:0000 до E000:0000 с шагом в 2Kb. Признаком наличия ПЗУ является наличие сигнатуры AA55 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. Такая процедура обычно используется для

инициализации дополнительных устройств. В Комплексе при выполнении этой процедуры проводится идентификация/аутентификация пользователя и контроль целостности, а при ошибке загрузка выполняться не будет.

Вся процедура идентификации/аутентификации и контроля целостности занимает 30-40 секунд (при контроле целостности файлов время увеличивается пропорционально количеству и размеру контролируемых файлов).

Устойчивость процедуры аутентификации зависит от длины пароля (см. Приложение Б). Допускается установка длины пароля от 0 до 12 символов.

При осуществлении контрольных процедур контроллер блокирует загрузку операционной системы с любых сменных носителей: флоппи-диска, CD-ROM и ZIP-drive, USB-disk и др.

После предъявления идентификатора выполняется процедура аутентификации (ввод пароля) пользователя. Для проведения процедуры аутентификации пароль вводится в виде символов <*>. Этим предотвращается возможность раскрытия индивидуального пароля и использования утраченного (похищенного) идентификатора.

С данными, полученными в результате идентификации/аутентификации пользователей, выполняется процедура хеширования. Таким образом, пароль пользователя не хранится в открытом виде даже в памяти контроллера.

Далее выполняется поиск свертки идентификационных параметров пользователя в базе данных контроллера. Если предъявлен зарегистрированный идентификатор, и пароль введен правильно, то выполняется контроль целостности защищаемых объектов.

При положительном результате контрольных процедур появляется сообщение «Доступ разрешен», и производится загрузка операционной системы. Если предъявленный пользователем идентификатор не зарегистрирован в списке (сообщения «Недопустимый идентификатор», «Ошибка чтения идентификатора») или нарушена целостность защищаемых объектов (сообщение «Нарушение целостности»), загрузка операционной системы не производится. Для продолжения работы потребуется вмешательство Администратора БИ.

Все программное обеспечение, реализующее контрольные процедуры (идентификация, аутентификация, проверка целостности), хранится в энергонезависимой памяти контроллера. Этим обеспечивается защита от разрушающих программных воздействий как встроенного программного обеспечения Комплекса, так и операционной системы и специального программного обеспечения Комплекса, размещаемых на жестком диске СВТ (РС).

После старта операционной системы управление передается «ядру защиты» Комплекса (монитор разграничения доступа).

Монитор разграничения доступа предназначен для разграничения доступа к ресурсам СВТ (АС) в соответствии с правилами разграничения доступа, назначенными Администратором БИ.

Дополнительно по завершении процесса загрузки ОС вызывается специальный PAM-модуль для проведения дополнительной идентификации и

аутентификации субъекта доступа в ОС. В случае успешной идентификации и аутентификации пользователя разрешается вход в ОС.

Каждому пользователю или группе пользователей Администратор БИ может назначить индивидуальный список файлов, которые будут контролироваться на целостность при входе данного пользователя в систему.

Механизм контроля целостности реализуется процедурой сравнения двух векторов для одного массива данных: эталонного (контрольного), выработанного заранее на этапе регистрации пользователей, и текущего, выработанного непосредственно перед проверкой.

Эталонный (контрольный) вектор вырабатывается на основе хэш-функций (контрольной суммы) защищаемых файлов и секретного ключа пользователя, который хранится в идентификаторе.

Важной составляющей безопасности при работе операционной системы является динамический контроль целостности процессов (задач) в оперативной памяти СВТ (РС). Администратор БИ может задать список процессов для динамического контроля, и в процессе функционирования Комплекса резидентная часть монитора разграничения доступа проверяет загружаемый процесс и обеспечивает оперативный контроль целостности исполняемых файлов перед передачей им управления. Тем самым обеспечивается защита от программных вирусов и закладок. В случае положительного исхода проверки управление передается операционной системе, и процесс запускается на исполнение. При отрицательном исходе проверки загрузка и запуск задачи не происходит.

Монитор разграничения доступа ограничивает доступ пользователя к ресурсам, расположенным как на локальных, так и на сетевых и сменных дисках, в соответствии с едиными правилами разграничения доступа.

Для защиты от извлечения платы контроллера Комплекса используется специальный механизм, обеспечивающий выполнение нормальной загрузки операционной системы только при наличии платы контроллера. При отсутствии платы контроллера загрузка операционной системы не выполняется.

8 ПОСТАВКА КОМПЛЕКСА

Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-Х» поставляется в составе:

1. СЗИ НСД «Аккорд-АМДЗ» в комплекте[5]:
   - контроллер «Аккорд» -1 шт.;
   - съемник информации (контактное устройство) - 1 шт.;
   - персональный идентификатор;
   - специальное программное обеспечение «Аккорд-Х» – на оптическом носителе;
   - эксплуатационная документация – на оптическом носителе;
   - формуляр на комплекс (37222406.26.20.40.140.080 ФО) – 1 брошюра;
   - комплект упаковки.

[5] тип контролера и его модификация, съемника информации, тип и количество персональных идентификаторов пользователей оговариваются при заказе Комплекса в соответствии с требованиями Заказчика и указываются в формуляре.

9 УСТАНОВКА И НАСТРОЙКА КОМПЛЕКСА

Установка Комплекса и его настройка с учетом особенностей политики информационной безопасности, принятой на объекте Заказчика, осуществляется, как правило, специалистами по защите информации организации (предприятия, фирмы и т.д.) в соответствии с требованиями эксплуатационной документации на Комплекс.

Установка Комплекса включает в себя:

1. Установку в СВТ (РС) аппаратной части Комплекса, его настройку с учетом конфигурации технических и программных средств СВТ (РС), в том числе регистрацию Администратора БИ (или нескольких администраторов) и пользователей. Установка и настройка Комплекса осуществляется Администратором БИ в соответствии с документом «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-X». Руководство администратора» (37222406.26.20.40.140.080 90);
2. Установку на жесткий диск СВТ (РС) специального программного обеспечения Комплекса и активизацию подсистемы разграничения доступа. Установка осуществляется Администратором БИ в соответствии с документом «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-X». Руководство администратора» (37222406.26.20.40.140.080 90);
3. Настройку защитных механизмов Комплекса в соответствии с правилами разграничения доступа к информации. Настройка осуществляется Администратором БИ в соответствии с документом «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-X». Руководство администратора» (37222406.26.20.40.140.080 90);
4. Реализацию организационных мер защиты, рекомендованных в эксплуатационной документации на Комплекс.

10 УПРАВЛЕНИЕ ЗАЩИТОЙ ИНФОРМАЦИИ

Созданная структура защиты информации при применении Комплекса должна поддерживаться механизмом установления полномочий пользователей СВТ (АС) и управлением их доступом к информационным ресурсам защищаемой АС.

Для этого на предприятии (учреждении, фирме и т.д.) должна создаваться служба безопасности информации или назначаться ответственное лицо (Администратор БИ), на которых возлагается разработка и ввод в действие организационно-нормативных документов по применению СВТ (АС) с внедренными средствами защиты Комплекса. Этими документами должно предусматриваться ведение ряда учетных и объектовых документов.

Перечень организационных мер, необходимых для обеспечения Комплексом требуемого уровня защиты информации, а также функции и обязанности Администратора БИ и пользователей приведены в документах «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-Х». Руководство администратора» (37222406.26.20.40.140.080 90) и «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-Х». Руководство оператора (пользователя)» (37222406.26.20.40.140.080 34).

11 ПРАВОВЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ КОМПЛЕКСА

«Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-Х» и сопутствующая документация защищены законом России об авторских правах, а также положениями Международного Договора. Любое использование Комплекса в нарушение закона об авторских правах или в нарушение положений эксплуатационной документации на Комплекс будет преследоваться предприятием-изготовителем в силу его возможностей.

Авторские права на данное изделие, в том числе аппаратные средства и специальное программное обеспечение, принадлежат ОКБ САПР, Россия, 113114, г. Москва, 2-й Кожевнический пер. д., 12, тел. +7 (926) 762-17-72 E-mail: okbsapr@okbsapr.ru.

Предприятие-изготовитель разрешает делать архивные копии программного обеспечения Комплекса для использования потребителем, который приобрел Комплекс в установленном порядке.

Ни при каких обстоятельствах программное обеспечение Комплекса не должно распространяться между другими предприятиями (фирмами) и лицами. Удалять в Комплексе уведомление об авторских правах ни при каких обстоятельствах не допускается.

При необходимости применения Комплекс для других целей, решение этого вопроса возможно только при наличии письменного согласия ОКБ САПР.

Отметим, что ограничения не запрещают Вам распространять Ваши собственные исходные коды или модули, связанные с применением программного обеспечения Комплекса. Однако тот, кто получает от Вас такие исходные коды или модули, должен приобрести собственную копию нашего программного обеспечения, чтобы на законном основании использовать его и иметь сертификат соответствия.

Относительно физических экземпляров аппаратуры и документации, поставляемых в составе Комплекса, предприятие-изготовитель гарантирует их исправность в соответствии с гарантийными обязательствами, указанными в документе «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-Х». Формуляр» (37222406.26.20.40.140.080 ФО).

При обнаружении ошибок или дефектов пользователь Комплекса должен направить в адрес предприятия-изготовителя подробный отчет о возникших проблемах, который позволит найти и зафиксировать проблему.

Комплекс поставляется по принципу «as is», т.е. предприятие-изготовитель ни при каких обстоятельствах не предусматривает никакой компенсации за Ваши дополнительные убытки, 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 Комплекса.

При покупке и применении Комплекса предполагается, что Вы знакомы с данными требованиями и согласны с положениями настоящего раздела.

12 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 адресам электронной почты: support@okbsapr.ru, help@okbsapr.ru.

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

ПРИЛОЖЕНИЕ А
МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ФОРМИРОВАНИЮ И ПОДДЕРЖКЕ ИЗОЛИРОВАННОЙ ПРОГРАММНОЙ СРЕДЫ (ИПС)

1. Методические рекомендации по формированию и поддержке изолированной программной среды (ИПС) разработаны с учетом следующих предположений.

В автоматизированной системе 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 (НСД) является использование имеющихся на жестком диске СВТ (РС) 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 при помощи имеющихся на СВТ (РС) или доставленных злоумышленником программных средств (в данном случае не рассматривается возможность нарушения целостности аппаратных средств компьютера).

НСД может носить непосредственный и опосредованный характер.

При непосредственном НСД злоумышленник, используя некоторое программное обеспечение 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 БИ 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 программным воздействиями (РПВ) или программными закладками. РПВ могут быть внедрены i-м пользователем в программное обеспечение, принадлежащее j-му пользователю только путем изменения программ, входящих в Tj.

Следовательно, система защиты от НСД 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 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 пользователя i должен обеспечивать выполнение программ только из подмножества Ti;
- пользователь не должен иметь возможности изменить подмножество Ti и/или исключить из дальнейшей работы защитный механизм и его отдельные части.

Положим, что в ПЗУ (BIOS) и операционной среде (в том числе и в сетевом программном обеспечении) отсутствуют специально интегрированные в них возможности НСД. Пусть пользователь работает с программой, в которой также исключено наличие каких-либо скрытых возможностей (проверенные программы). Потенциально злоумышленные действия могут быть такими:

а) Проверенные программы будут использованы на другой СВТ (PC) с другим BIOS и в этих условиях использоваться некорректно;

б) Проверенные программы будут использованы в аналогичной, но не проверенной операционной среде, в которой они также могут использоваться некорректно;

в) Проверенные программы используются на проверенной СВТ (PC) и в проверенной операционной среде, но запускаются еще и не проверенные программы, потенциально несущие в себе возможности НСД.

Тогда, несанкционированный доступ в АС гарантированно невозможен, если выполняются условия:

- У1. На СВТ (PC) с проверенным BIOS установлена проверенная операционная среда;
- У2. Достоверно установлена неизменность BIOS для данного сеанса работы;
- У3. Кроме проверенных программ в данной программно-аппаратной среде не запускалось и не запускается никаких иных программ, кроме проверенных на целостность перед запуском;
- 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.

Функционирование программ в изолированной программной среде существенно ослабляет требования к базовому программному обеспечению. В самом деле, 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 программного обеспечения требуется только:

- Невозможность запуска программ помимо контролируемых ИПС событий;
- Отсутствие в базовом программном обеспечении возможностей влиять на среду функционирования уже запущенных программ (фактически это требование невозможности редактирования оперативной памяти).

Все прочие действия, являющиеся нарушением Условий 1-3, в оставшейся их части будут выявляться и блокироваться.

Таким образом, ИПС существенно снижает требования к программному обеспечению в части наличия скрытых возможностей.

Основным элементом поддержания изолированной программной 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 разрушающее программное воздействие 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 разрушающее программное воздействие может влиять на процесс чтения-записи данных на уровне файлов или на уровне секторов и предъявлять системе контроля некоторые другие вместо реально существующих данных. Этот механизм неоднократно реализовывался в STELTH-вирусах. Однако верно утверждение - если программный модуль, обслуживающий процесс чтения данных, не содержал разрушающее программное воздействие и целостность его зафиксирована, то при его последующей неизменности чтение с использованием этого программного модуля будет чтением реальных данных. Из данного утверждения следует, что для обеспечения чтения реальных данных (защиты от разрушающего программного воздействия подсистема контроля целостности Комплекса должна строиться на основе алгоритма ступенчатого (пошагового) контроля целостности.

Алгоритм ступенчатого контроля целостности для создания ИПС приведен на примере DOS.

При включении питания СВТ (PC) происходит тестирование оперативной памяти, 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 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 операционную 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 запуска программ и контроля целостности.

2. Реализация ИПС с использованием механизма расширения BIOS

2.1. Рассмотрим два этапа реализации ИПС - этап установки ИПС и этап эксплуатации ИПС.

Предположим существование N пользователей, каждый i-й из которых характеризуется некоторой персональной информацией Ki, не известной другим пользователям и хранящейся на некотором материальном носителе (например, устройстве типа Touch Memory). Существует также Администратор БИ, который знает все Ki и единолично проводит этап установки. Пользователи же участвуют только на этапе эксплуатации.

2.2. Процесс установки ИПС состоит из следующих действий:

а) В СВТ (PC) устанавливается плата, включающая в себя устройства и программы ПЗУ данного устройства, реализующие:

- чтение Ki,
- идентификацию пользователя с номером i по введенному Ki,
- чтение массива данных, содержащего множество доступных для выполнения пользователем i задач Pi1, Pi2, ..., Pim, и информации Mi1, Mi2, ... Mim, фиксирующей целостность файлов Fi1, ..., Fim каждой задачи.

Описанное устройство должно активизироваться сразу после включения питания, отработки процедур самотестирования и инициализации системы прерываний.

Для СВТ (PC) типа IBM PC для этой цели необходимо использовать механизм расширения BIOS.

б) Администратор БИ определяет для пользователя i набор задач и соответствующих задачам исполняемых файлов {Pit, Fit}, t=1,...,mi; i=1, ..., N, где mi - число разрешенных к запуску задач для i-го пользователя.

в) Администратор БИ формирует (и заносит на носитель) или считывает с носителя для i-го пользователя его Ki и вычисляет значения для последующего контроля целостности Mir= f(Ki, Fir, Pir), где f - функция фиксации целостности (хэш-функция).

г) Администратор проделывает действия б) и в) для всех N пользователей.

д) Администратор БИ устанавливает в программную среду модуль активизации ИПС и фиксирует его целостность. Фиксируется также целостность файлов операционной среды Foc, в которые входят файлы DOS, драйверы и сетевое программное обеспечение.

2.3. Процесс эксплуатации состоит из следующих действий:

- Включение питания и активизация расширенного BIOS;
- Запуск каждого процесса.

2.3.1. Включение питания и активизация расширенного BIOS состоит из следующих действий:

а) идентификация пользователя по его Ki. При успехе выполняется п. 2.3.1.б);

б) проверка целостности всех включенных в СВТ BIOS При положительном исходе выполняется п. 2.3.1.в);

в) чтение файлов Fипс и Fос с помощью функций операционной среды и проверка их целостности. При положительном исходе выполняется п. 2.3.1.г).

г) активизация операционной системы и сетевого программного обеспечения;

д) активизация процесса контроля Рипс;

е) Запуск избранной задачи i-го пользователя.

2.3.2. Запуск каждого процесса Ps сопровождается проверками:

а) принадлежит ли Fs к множеству разрешенных для i (Ti), если да, то выполняется п. 2.3.2.б), иначе запуск игнорируется;

б) совпадает ли G=f(Ki,Fs,Ps) с M=f(Ki,Fs,Ps), назначенными Администратором БИ;

в) при положительном исходе проверки по п. 2.3.2.б) задача запускается.

Условия изолированности среды (У1-5) в данном случае будут выполнены, так как:

- выполнение условия У1 гарантируется при установке системы Администратором БИ;
- выполнение условий У2, У4 и У5 обеспечиваются контроллером Комплекса (загрузка операционной системы с других магнитных носителей невозможна, поскольку расширенный BIOS активен раньше и направляет загрузку на жесткий диск; пользователь допускается к работе только при проверке Ki);
- выполнение условия У3 обеспечивается программным модулем контроля запусков и контроля целостности задач, входящим в состав Комплекса. Кроме того, в данном случае реализован механизм ступенчатого контроля, обеспечивающий чтение реальных данных.

ПРИЛОЖЕНИЕ Б.
МЕТОДИКА ОЦЕНКИ ДЛИНЫ ПАРОЛЯ, ИСПОЛЬЗУЕМОГО ПРИ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ

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 БИ.

Пусть требуемая вероятность подбора пароля в результате трехмесячного регулярного тестирования должна быть не выше 0,001. По формуле Андерсона (см. Хоффман Л. Современные методы защиты информации /Пер.с англ./, М.: Советское радио, 1980, - 264с.) должно выполняться условие:

$$4{,}32 * 10^{**}4 * k(M/P) <= A^{**}S, \text{ где:}$$

k - количество попыток в мин;

M - период времени тестирования в месяцах;

P - вероятность подбора пароля;

A - число символов в алфавите;

S - длина пароля.

Время на одну попытку при использовании Комплекса - не менее 7 сек., т.е.

$$k = 60/7 = 8{,}57$$

Для английского алфавита A=26.

Принимаем S=7.

Тогда условие по формуле Андерсона выполняется.

$$1{,}11 * 10^{**}9 <= 8{,}03 * 10^{**}9$$

Таким образом, пароля длиной 7 символов достаточно для выполнения условия (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:

$$3{,}7 * 10^{**}8 * M <= 3{,}089 * 10^{**}8, \text{ или } M <= 0{,}83$$

При длине пароля 6 символов и регулярном тестировании в течение 25 дней вероятность подбора пароля составит не более 0,001.

ПРИЛОЖЕНИЕ В. АЛГОРИТМ ВЫЧИСЛЕНИЯ ХЭШ-ФУНКЦИИ, ПРИМЕНЯЕМЫЙ В КОМПЛЕКСЕ

В Комплексе применяется специальный алгоритм вычисления хэш-функции.

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]), 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 длины 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.

Начальное состояние регистра H предлагается следующее:

6B 9D D4 57 CD F6 EA 58 E7 63 5B C5 27 FA 5F 9A D3

Состояние регистра H после обработки одного блока текста является начальным для обработки следующего. Состояние регистра H после обработки последнего блока объявляется сверткой текста.

При обработке одного блока схема работает 48 тактов. Первые 16 тактов для функции обратной связи регистра H выбирается f[0], следующие 16 тактов - f[1], следующие 16 тактов - f[2].