ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН
11443195.4012-037 31-ЛУ

Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «АККОРД-Win64» (версия 5.0)

ОПИСАНИЕ ПРИМЕНЕНИЯ

11443195.4012-037 31

АННОТАЦИЯ

Настоящий документ является описанием применения программно-аппаратного комплекса средств защиты информации от НСД «Аккорд-Win64» v.5.0 (ТУ 4012-037-11443195-2010), далее комплекс «Аккорд», ПАК СЗИ НСД «Аккорд» либо комплекс, предназначенного для лиц, планирующих и организующих защиту информации в системах и средствах информатизации на базе СВТ.

В документе приведены нормативные требования по защите информации, общие принципы и правила организации работы по обеспечению конфиденциальности информации, основные защитные функции комплекса, его возможности, особенности установки и применения.

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

Применение защитных механизмов комплекса «Аккорд» должно дополняться общими мерами предосторожности и физической безопасности СВТ.

СОДЕРЖАНИЕ

1. Нормативные требования по защите информации 4
1.1. Необходимость и цели защиты информации 4
1.2. Основные принципы организации защиты информации от НСД и обеспечения ее конфиденциальности 5
2. Общие сведения 7
3. Технические требования и организационные меры, необходимые для применения комплекса 9
3.1. Технические требования 9
3.2. Организационные меры 10
4. Особенности защитных функций комплекса 11
5. Построение системы защиты информации на основе комплекса 14
5.1. Подсистема управления доступом 15
5.2. Подсистема регистрации и учета 15
5.3. Подсистема обеспечения целостности 16
5.4. Открытый интерфейс для подключения СКЗИ 17
6. Состав комплекса 18
6.1. Аппаратные средства 18
6.2. Программные средства 19
7. Принцип работы комплекса 23
8. Поставка комплекса 26
9. Установка и настройка комплекса 27
10. Управление защитой информации 28
11. Правовые аспекты применения комплекса 29
Приложение 1. Методические рекомендации по формированию и поддержке изолированной программной среды (ИПС) 31
Приложение 2. Методика определения требуемой (целесообразной) длины пароля, используемого в комплексах СЗИ НСД семейства «Аккорд»™ при аутентификации пользователей 36

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 (НД БИ);
- реализация мер защиты в соответствии с потребностями владельцев (пользователей) информации.

В соответствии с п. 4 статьи 16 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации»:

«Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации».

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 и обеспечения ее конфиденциальности

Мероприятия по защите информации от НСД являются составной частью управленческой, научной, производственной (коммерческой) 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 АС должна учитывать следующие принципы и правила обеспечения безопасности информации[1]:

1) 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.

2) Выявление конфиденциальной информации и документальное оформление в виде перечня сведений, подлежащих защите, его своевременная корректировка.

3) Наиболее важные решения по защите информации должны приниматься руководством предприятия (организации, фирмы), владельцем АС.

4) Определение уровней полномочий субъектов доступа, а также круга лиц, которым предоставлено право присвоения уровней полномочий.

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

6) 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;
- определение уровня полномочий в соответствии с его должностными обязанностями;

---

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

- получения от субъекта доступа расписки о неразглашении доверенной ему конфиденциальной информации.

7) Обеспечение физической охраны объекта информатизации, на котором расположена защищаемая АС (территория, здания, помещения, хранилища 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.

8) Организация службы безопасности информации (ответственные лица, администраторы БИ), осуществляющей учет, хранение и выдачу информационных носителей, паролей, ключей, ведение служебной информации СЗИ НСД (генерацию 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.

9) Планомерный и оперативный контроль уровня безопасности защищаемой информации согласно НД по безопасности информации, в т.ч. проверка защитных функций средств защиты информации.

10) Средства защиты информации должны иметь СЕРТИФИКАТ, удостоверяющий их соответствие требованиям по безопасности информации.

2. Общие сведения

Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-Win64» v.5.0 (далее по тексту – ПАК СЗИ НСД «Аккорд» или комплекс «Аккорд») предназначен для применения на СВТ, функционирующих под управлением 64-bit Windows XP, Windows Server 2003, Windows Vista, Windows 2008, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 с целью обеспечения защиты от несанкционированного доступа к СВТ и АС на их основе при многопользовательском режиме эксплуатации.

Комплекс СЗИ НСД «Аккорд» включает:

- программно-аппаратный комплекс СЗИ НСД «Аккорд-АМДЗ» (ТУ 4012-006-11443195-97 03);
- специальное программное обеспечение разграничения доступа в среде операционных систем Windows, построенных с использованием технологии NT – СПО «Аккорд-Win64» (версии 5.0).

В составе комплекса «Аккорд» могут применяться различные модификации специализированных контроллеров:

- контроллер «Аккорд-5МХ» используется для защиты СВТ с шинным интерфейсом PCI (3.3В, 5В) или PCI-X (3.3В);
- контроллер «Аккорд-5.5» используется для защиты СВТ с шинным интерфейсом PCI (5В), или PCI-X (3.3В);
- контроллеры «Аккорд-5.5е», «Аккорд-GX» используются для защиты СВТ с шинным интерфейсом PCI-Express;
- контроллеры «Аккорд-GXM», «Аккорд-GXMH» используются для защиты СВТ с шинным интерфейсом miniPCI-Express;
- контроллер «Аккорд-GXM2» используется для защиты СВТ с шинным интерфейсом M.2 с ключами A и/или E (интерфейс PCI-Express).

Все модификации вышеуказанных контроллеров:

- могут использоваться на СВТ с процессором и объемом RAM, обеспечивающим применение 64-bit ОС Windows XP/2003/Vista/2008/7/8/2008 R2/8.1/10/2012/2012 R2;
- используют для идентификации пользователей персональные идентификаторы TM DS 1992-1996, USB-устройства ШИПКА, eToken Pro, eToken (Java), Рутокен Lite, Рутокен ЭЦП 2.0, Рутокен S;
- используют для аутентификации пароль до 12 символов. В процессе аутентификации дополнительно проверяется значение ключа, записанного в память идентификатора;
- блокируют загрузку СВТ любых внешних носителей;
- обеспечивают многопользовательский режим эксплуатации СВТ с возможностью регистрации (в энергонезависимой памяти) до 126 пользователей на одной ПЭВМ (для моделей на базе специализированных контроллеров семейства «Аккорд-5МХ/5.5») и до 1022 поль-

зователей на одной ПЭВМ (для моделей на базе специализированных контроллеров семейства «Аккорд-LE/GX»);

- имеют аппаратный датчик случайных чисел (ДСЧ) для криптографических приложений;
- обеспечивают контроль целостности программ, данных, системных областей жестких дисков, разделов и ключей системного реестра, а также конфигурации технических средств СВТ до загрузки ОС;
- имеют внутреннюю энергонезависимую память для хранения данных о зарегистрированных пользователях и журнала регистрации событий;
- допускают изменение встроенного ПО (технологический режим) без замены аппаратной части комплекса (платы контроллера);
- обеспечивают режим доверенной загрузки ОС (выполнение процедур идентификации/аутентификации пользователя, контроль целостности аппаратной части СВТ, системных файлов, программ и данных на аппаратном уровне до загрузки ОС);
- допускают очистку баз данных в энергонезависимой памяти (повторную инициализацию) без вскрытия системного блока.

Состав комплекса «Аккорд» (тип контроллера и съемника информации (контактного устройства), тип и количество идентификаторов) определяется при заказе комплекса в соответствии с требованиями Заказчика и указывается в формуляре.

3. Технические требования и организационные меры, необходимые для применения комплекса

3.1. Технические требования

Для установки комплекса «Аккорд» требуется следующий минимальный состав технических и программных средств:

- установленная на СВТ 64-bit операционная система Windows XP, Windows Server 2003, Windows Vista, Windows 2008, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2;
- наличие CD ROM для установки СПО разграничения доступа;
- наличие USB-разъема[2];
- наличие считывателя смарт-карт[3];
- объем дискового пространства для установки СПО разграничения доступа – не менее 11 Мб;
- наличие соответствующего свободного слота на материнской плате СВТ для установки контроллера комплекса «Аккорд-АМДЗ» (в зависимости от типа специализированного контроллера).

При применении комплекса «Аккорд» количество пользователей, регистрируемых на одном СВТ, не должно превышать 126 человек (для моделей на базе специализированных контроллеров семейства «Аккорд-5МХ/5.5»), так как объем энергонезависимой памяти контроллеров комплекса СЗИ НСД «Аккорд-АМДЗ» позволяет хранить данные на такое количество идентификаторов. При использовании комплекса для защиты систем терминального доступа, когда синхронизация с АМДЗ отключена, возможна регистрация до 1024 пользователей.

Количество и тип идентификаторов, используемых для идентификации пользователей средствами комплекса СЗИ НСД «Аккорд-АМДЗ» из состава комплекса «Аккорд-Win64» v.5.0, определяется Заказчиком при поставке и указывается в формуляре.

Аппаратные средства, используемые в составе комплекса «Аккорд» проверены на совместимость практически со всем доступным разработчику программно-аппаратным обеспечением СВТ как зарубежного, так и отечественного производства. Совместимость обеспечивается правильной установкой и настройкой комплекса.

[2)] В случае использования в качестве идентификатора устройства ШИПКА или ТМ-считывателя с интерфейсом USB

[3)] В случае использования смарт-карт в качестве идентификатора

3.2. Организационные меры[4]

Для эффективного применения средств защиты комплекса и поддержания необходимого уровня защищенности СВТ и информационных ресурсов АС **необходимы:**

- физическая охрана СВТ и его средств, в том числе проведение мероприятий по недопущению изъятия контроллера комплекса СЗИ НСД;
- наличие администратора безопасности информации (супервизора) - привилегированного пользователя, имеющего особый статус и абсолютные полномочия. 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 за правильным использованием 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 (11443195.4012-037 90);
- использование в СВТ технических и программных средств, сертифицированных как в Системе ГОСТ Р, так и в ГСЗИ;
- запрет на использование в СВТ любых сторонних служб и протоколов, позволяющих осуществить удаленный доступ к подконтрольным объектам (Telnet, SSH, TeamView, RemoteDesktop и т.д.).

[4] более подробно приведены в «Руководстве администратора» (11443195.4012-037 90) и «Руководстве оператора» (Пользователя), 11443195.4012-037 34 и других документах ЭД на комплекс.

4. Особенности защитных функций комплекса

Комплекс СЗИ НСД «Аккорд» обеспечивает защиту информации по 3-му классу для СВТ[5] и возможность использования для защиты информации в АС до классов защищенности 1Б, 2А, 3А и в ИСПДн до 1 класса включительно, без изменения ранее приобретенных программных средств.

Защитные функции комплекса реализуются применением:

1)дисциплины защиты от НСД СВТ, включая:

- идентификацию пользователя по уникальному Идентификатору;
- аутентификацию с учетом необходимой длины пароля и времени его жизни;
- аппаратный (до загрузки ОС) контроль целостности технических средств СВТ, программ и данных на жестком диске (в том числе системных областей диска и модулей программной части комплекса);
- ограничение времени доступа субъекта к СВТ в соответствии с установленным режимом работы пользователей;
- блокировку несанкционированной загрузки СВТ с отчуждаемых носителей (FDD, CD-ROM, ZIP-drive, USB-disk и др.);

2)процедур блокирования экрана и клавиатуры по команде пользователя или по истечению установленного интервала «неактивности» пользователя;

3)дисциплины разграничения доступа к локальным и сетевым ресурсам СВТ в соответствии с установленными ПРД и определяемыми атрибутами доступа (подробнее см. документ «Установка правил разграничения доступа. Программа ACED32» пункт 6.10), которые устанавливаются администратором БИ в соответствие каждой паре «субъект доступа - объект доступа» при регистрации пользователей.

Комплекс СЗИ НСД «Аккорд» позволяет администратору использовать как дискреционный, так и мандатный методы разграничения доступа. При использовании мандатного доступа с контролем процессов (исполняемых модулей) выполняется процедура управления потоками информации. Администратор может предоставить пользователю выбор уровня доступа запускаемой задачи, или выбор уровня конфиденциальности всей сессии пользователя. Данный механизм позволяет обрабатывать документы разного уровня конфиденциальности одним набором прикладного ПО без ухудшения надежности защитных механизмов.

4)дисциплины управления процедурами ввода/вывода на отчуждаемые носители информации. Дополнительно для каждого пользователя контролируется список разрешённых USB-устройств и SD карт в соответствии с их уникальными идентификационными номерами;

5)дисциплины контроля доступа к любому устройству, или классу устройств, доступных в «Диспетчере устройств» Windows, в том числе последо-

---

[5] по классификации РД. Сборник руководящих документов по защите информации от несанкционированного доступа. - М.: Гостехкомиссия России, 1998

вательных и параллельных портов, устройств PCMCI, IEEE 1394, WiFi, Bluetooth и пр;

6)дисциплины гарантированной очистки оперативной памяти и остаточной информации на жестких дисках и внешних носителях;

7)дисциплины контроля вывода на печать документов из любых программ и программных пакетов и автоматической маркировки печатных листов специальными пометками, грифами и т.д. Процесс печати протоколируется в отдельном журнале (создаётся учетная карточка документа);

8)регистрации контролируемых событий, в том числе несанкционированных действий пользователей, в системном журнале, доступ к которому предоставляется только Администратору БИ;

9)дисциплины защиты от НСД систем терминального доступа, функционирующих на базе терминальных служб сетевых операционных систем Windows и программного обеспечения компании Citrix Systems для терминальных серверов;

10) 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, а далее с периодичностью, заданной администратором), так и динамический список, проверка по которому выполняется при каждой загрузке контролируемого файла в оперативную память. Для статического контроля администратор может включить дополнительную функцию восстановления поврежденного файла;

11) дисциплины функционального замыкания информационных систем, т.е. создания изолированной программной среды за счет использования защитных механизмов комплекса;

12) возможности встраивания или совместного использования других средств защиты информации, в том числе криптографических;

13) других механизмов защиты в соответствии с требованиями нормативных документов по безопасности информации;

Комплекс «Аккорд» может применяться в произвольной и функционально изолированной программной среде, обеспечивая при этом:

- защиту от несанкционированного доступа к СВТ и их ресурсам;
- разграничение доступа к ресурсам СВТ, 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;
- функциональное замыкание информационных систем с исключением возможности несанкционированного входа в ОС и загрузки с внешнего носителя;

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

В комплексе «Аккорд» используются и некоторые дополнительные механизмы защиты от НСД к СВТ. Так, в частности, для пользователя администратор БИ может установить:

- время жизни пароля и его минимальную длину, практически исключив тем самым возможность быстрого его подбора (Приложение 3);
- временные ограничения использования СВТ для пользователей путем определения и установки администратором БИ интервала времени по дням недели (с дискретностью 30 мин), в котором разрешена работа для данного пользователя;
- параметры управления экраном – гашение экрана через заранее определенный интервал времени (в случае, если в течение указанного интервала действия оператором не выполнялись). Возможность продолжения работы предоставляется только после проведения повторной идентификации по персональному Идентификатору пользователя;
- подачу соответствующих звуковых и визуальных сигналов при попытках несанкционированного доступа к СВТ и к их ресурсам.

ВНИМАНИЕ! Применение комплексов СЗИ НСД семейства «Аккорд»™ совместно с сертифицированными программными средствами криптографической защиты информации (СКЗИ) позволяет значительно снизить нагрузку на организационные меры, определенные условиями применения этих средств. При этом класс защищенности не снижается.

5. Построение системы защиты информации на основе комплекса

Построение системы защиты информации с использованием комплекса «Аккорд» и ее взаимодействие с программно-аппаратным обеспечением СВТ показаны на рисунке 1.

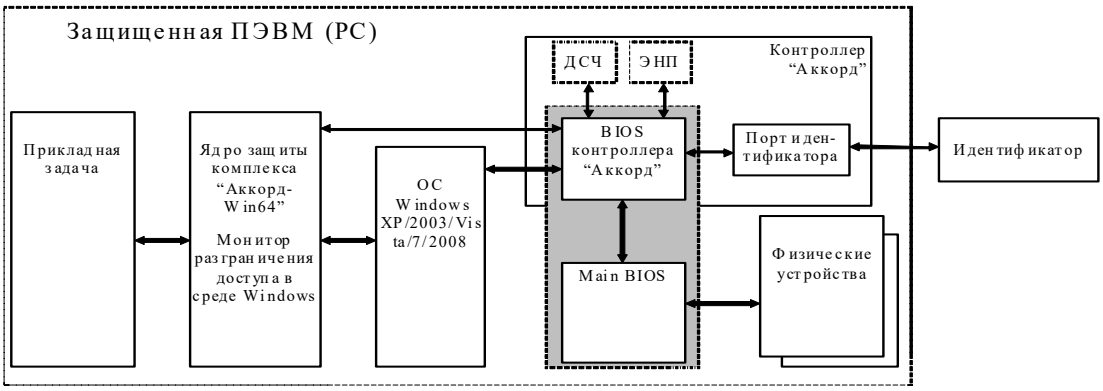

Рисунок 1 - Построение системы защиты информации с использованием комплекса «Аккорд»

Защита информации с использованием средств комплекса основана на обработке событий, возникающих при обращении прикладных программ или системного ПО 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 «Аккорд» состоит из собственно средств защиты СВТ от НСД и средств разграничения доступа к ее ресурсам, которые условно можно представить в виде четырех взаимодействующих между собой подсистем (рисунок 2) защиты информации.

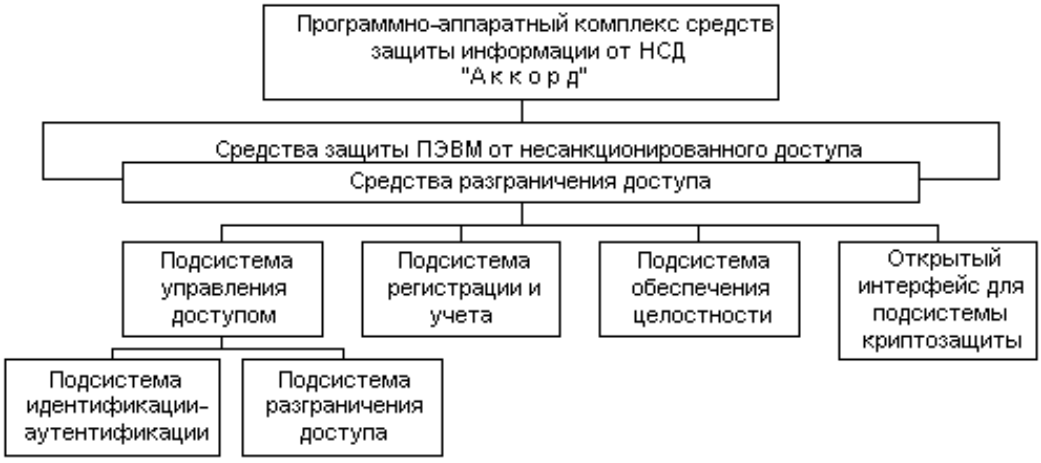

Рисунок 2 – Состав комплекса «Аккорд»

5.1. Подсистема управления доступом

Предназначена для защиты СВТ от посторонних[6] пользователей, управления доступом к объектам доступа и организации совместного их 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 принадлежности данного идентификатора данному пользователю) с защитой от раскрытия пароля. Для идентификации/аутентификации пользователей используются персональные идентификаторы DS-1992-1996 (Touch memory-«Память касания»), USB идентификаторы ШИПКА, eToken Pro, eToken (Java), Рутокен Lite, Рутокен ЭЦП 2.0, Рутокен S.

В комплексе «Аккорд» реализованы принципы дискреционного и мандатного управления доступом. При использовании дискреционного управления 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 пользователю (субъекту) устанавливается уровень доступа, а объекту (данным или задаче) 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 программы ACED32, см. документ «Установка правил разграничения доступом. Программа ACED32» (11443195.4012-037 97), входящий в состав эксплуатационной документации на комплекс.

5.2. Подсистема регистрации и учета

Предназначена для регистрации в системном журнале событий, обрабатываемых комплексом СЗИ НСД «Аккорд-АМДЗ» и подсистемой разграничения доступа «Аккорд-Win64» v.5.0. При регистрации событий в системном журнале указываются:

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

Перечень регистрируемых событий, их описание приводится в «Руководстве администратора» (11443195.4012-037 90).

Работа с системными журналами осуществляется с использованием программы LOGVIEW.EXE, см. документ «Подсистема регистрации. Программа рабо-

[6] Под посторонними пользователями понимаются все лица, не зарегистрированные в системе (не имеющие зарегистрированного в конкретном СВТ Идентификатора)

ты с журналами регистрации «LogView» (11443195.4012-037 99) из комплекта эксплуатационной документации на комплекс.

ВНИМАНИЕ! Доступ к системному журналу возможен только для администратора БИ (супервизора).

5.3. 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:

- проверкой целостности конфигурации технических средств СВТ перед каждым сеансом работы пользователя;
- проверкой целостности назначенных для контроля системных файлов, пользовательских программ и данных;
- исключением возможности использования СВТ без контроллера комплекса;
- механизмом создания изолированной программной среды, запрещающей запуск неразрешенных программ.

Функционирование подсистемы обеспечения целостности в комплексах СЗИ НСД семейства «Аккорд» 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 не обнаружения модификации файла используется сложный алгоритм расчета контрольных сумм.
- защита от модификации программы расчета контрольной суммы обеспечивается тем, что она хранится в памяти контроллера комплекса;
- при контроле целостности индивидуального списка файлов пользователя результирующая КС хранится на жестком диске, но в алгоритме расчета используется ключ пользователя, записанный в идентификаторе;
- секретный ключ пользователя формируется из последовательности случайных чисел и записывается в идентификатор пользователя при регистрации. Этот ключ используется при выработке КС и исключает возможность несанкционированной модификации файлов из индивидуального списка контролируемых файлов.

5.4. Открытый интерфейс для подключения СКЗИ

Обеспечивает возможность применения комплекса совместно с сертифицированными средствами криптографической защиты информации (СКЗИ). При этом обеспечивается выработка случайных последовательностей с помощью двухканального аппаратного ДСЧ, смонтированного на плате контроллера комплекса.

6. Состав комплекса

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

6.1. Аппаратные средства

Комплекс «Аккорд» включает в себя аппартные средства «Аккорд-АМДЗ» (ТУ 4012-006-11443195-97):

- одноплатный контроллер, устанавливаемый в свободный слот материнской платы СВТ. Характеристика контроллеров комплекса СЗИ НСД «Аккорд-АМДЗ» приведена в таблице 1.
- съемник информации с контактным устройством (11443195.4012-006 93), обеспечивающий интерфейс между контроллером комплекса и персональным идентификатором пользователя.

Съемник информации может быть внешним – соединительный провод находится вне корпуса СВТ и подключение осуществляется к задней планке контроллера посредством разъема RJ-11, и внутренним – соединительный провод находится внутри корпуса СВТ, подключение осуществляется с помощью разъема, находящегося на плате контроллера «Аккорд».

Контактное устройство внешних съемников крепится в удобном для пользователя месте (на корпусе СВТ, 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, с помощью гайки, либо пружинной или резиновой шайбы.

- персональный идентификатор пользователя DS 1992-1996 (11443195.4012-006 94). Представляет собой полупассивное микропроцессорное устройство, снабженное элементом питания, в виде «таблетки» диаметром 16 мм и толщиной 3-5 мм в удобной пластмассовой (металлической) оправке. Каждый ТМ-идентификатор обладает уникальным номером (48 бит), который формируется технологически и подделать который практически невозможно. Объем памяти, доступной для записи и чтения составляет до 64 Кбит в зависимости от типа идентификатора. Срок хранения записанной информации, обеспечиваемый элементом питания, - не менее 10 лет.
- При монтаже на плате контроллера USB-порта в качестве идентификатора может использоваться USB устройство ШИПКА производства ОКБ САПР, а контактным устройством служит специализированный кабель.

Модификация контроллера и съемника информации с контактным устройством комплекса СЗИ НСД «Аккорд-АМДЗ», количество и тип идентификаторов пользователей и оговаривается в соответствии с требованиями Заказчика при поставке комплекса и указываются в формуляре.

6.2. Программные средства

Программные средства комплекса «Аккорд» включают:

- Программные средства комплекса СЗИ НСД «Аккорд-АМДЗ» – встраиваемое программное обеспечение (11443195.4012-006 12 0x)[1];
- Служебные (сервисные) программы комплекса СЗИ НСД «Аккорд-АМДЗ»[2].

Таблица 1 - Служебные (сервисные) программы комплекса СЗИ НСД «Аккорд-АМДЗ»[3]

Имя файла	Назначение файла
IP55.EXE	Программа очистки базы данных пользователей в ЭНП контроллера «Аккорд-5.5»
IP5x.EXE	Программа очистки базы данных пользователей в ЭНП контроллера «Аккорд-5mx»
BIOS	Папка с внутренним ПО контроллеров АМДЗ
DRIVERS	Папка с драйверами устройств (контроллеров «Аккорд»)

Специальное ПО разграничения доступа в среде Windows в составе:

- ядро защиты – программы, реализующие защитные функции комплекса;
- программы управления защитными функциями комплекса (настройки комплекса в соответствии с ПРД);

Таблица 2 - Состав СПО «Аккорд-Win64» v.5.0 (11443195.4012-037 12)

Функциональное назначение программ	Наименование модуля	Назначение и краткая характеристика модуля
	ACRUN.SYS.	Ядро системы, выполненное как kernel mode driver. Реализует функции монитора разграничения доступа и обеспечивает статический и динамический контроль целостности файлов/исполняемых модулей. Так же он реализует функции хранителя экрана.

[1] размещается в ЭНП контроллера на предприятии-изготовителе при изготовлении комплекса

[2] поставляется на дискете с ЭД на комплекс «Аккорд-АМДЗ», или на компакт-диске

[3] поставляется на дискете с ЭД на комплекс «Аккорд-АМДЗ», или на компакт-диске

Функциональное назначение программ	Наименование модуля	Назначение и краткая характеристика модуля
Ядро защиты[4]	ACGINA.DLL	Программа, реализующая процедуры идентификации/аутентификации Windows NT, так называемые, процедуры winlogon. Представляет собой модификацию (wraper) стандартной библиотеки msgina.dll. Эта программа необходима для входа в систему с идентификационными параметрами, полученными из контроллера комплекса «Аккорд-АМДЗ», отслеживания завершения сеанса работы пользователя, а также начала нового сеанса работы. Так же, выполняет функции вывода на экран информации, поступающей от ACRUN.SYS.
	ACED32.EXE	Программа-редактор прав доступа пользователей к объектам ОС. Позволяет редактировать список пользователей, формировать ПРД для конкретного пользователя (используя дискреционную или мандатную модель доступа), назначить дополнительные параметры.
	ACUSRMOD.DLL	Библиотека для перехвата работы с клипбордом и принтерами
Программы управления (настройки)	ACED32N.HLP	Справка для программы ACED32.EXE
	ACCORD.INI	Файл, содержащий описание конфигурации и настроек системы в целом
	ACHOOKMK.DLL	Библиотека, осуществляющая блокировку компьютерной мыши и клавиатуры СВТ, оснащенного ОС Windows Server 2008/ Windows Server 2012, в режиме терминальной сессии
	LOGVIEW.EXE	Программа просмотра, фильтрации, вывода на печать журналов работы пользователей
	LOGBASE.EXE	Программа для управления журналами пользователей (сортировка по пользователям, по датам, работа с архивами журналов).
	LOGTOPRD.EXE	Программа для анализа журналов пользователей и составления ПРД по результатам анализа.
	ACRUNNT.EXE.	Исполняемый модуль монитора разграничения доступа. Обеспечивает сервис, необходимый для вывода на экран логотипа фирмы, блокирования экрана с помощью мыши и вывода сообщений от ACRUN.SYS.
	ACSETUP.EXE	Программа активизации подсистемы разграничения доступа. Осуществляет установку/снятие программной части системы защиты комплекса, а также изменение параметров её функционирования
	USRTOAZ.DLL	Библиотека синхронизации баз пользователей АМДЗ и ACED32. Используется программой ACED32.EXE.

[4] В связи со значимостью функций, выполняемых этой частью программного обеспечения, необходимо выполнение контроля целостности до загрузки ОС с помощью внутреннего ПО контроллера «Аккорд». Рекомендуемый список контролируемых файлов приводится в документе «Руководство администратора» (11443195.4012-036 90)

Функциональное назначение программ	Наименование модуля	Назначение и краткая характеристика модуля
	AZIAHLP.DLL	Библиотека, осуществляющая работу с базой данных пользователей в ЭНП контроллера «Аккорд-АМДЗ». Используется библиотекой USRTOAZ.DLL.
	AMZTONT.DLL	Библиотека, осуществляющая синхронизацию базы данных пользователей АМДЗ и учётных записей Windows NT. Используется программой ACED32.EXE
	TMATTACH.DLL	Библиотека, содержащая графическое представление работы с TouchMemory. Используется программой ACED32.EXE.
	TMDRV32.DLL	Библиотека, осуществляет связь с драйвером контроллера комплекса «Аккорд-АМДЗ» и служит для работы с Touch Memory. Используется библиотекой TMATTACH.DLL.
	TMEXPLOR.EXE	Тестовая программа, служащая для проверки работоспособности платы комплекса «Аккорд АМДЗ»
	UNZDLL.DLL	Библиотека разархивирования. Используется программой LOGBASE.EXE.
	ZIPDLL.DLL	Библиотека архивирования. Используется программой LOGBASE.EXE.
	EDS32.DLL	Библиотека вычисления КС. Используется программой ACED32.EXE.
	AZLOG.DLL	Библиотека доступа к журналу АМДЗ из программы LOGVIEW.EXE
	ACPRNCFG.EXE	Программа настройки параметров маркировки печати документов.
	ACTSKMNG.EXE	Программа менеджера задач, доступных для запуска пользователем в изолированной среде.
	MAKEPRC.EXE	Программа создания и корректировки списка исключительных процессов.
	ACXALLOW.SYS	Драйвер контроля имён общих ресурсов[5]
	ACXLMSRV.SYS	Драйвер контроля доступа из сети к ресурсам компьютера, выделенным в общий доступ
	ACBOOT.SYS	Драйвер для поддержки USB-клавиатуры. Используется драйвером ACRUN.SYS
	ACLOCKNT.SYS	Драйвер блокировки клавиатуры и мыши в ОС Windows NT. Используется драйвером ACRUN.SYS
	ACLOCK2K.SYS	Драйвер блокировки клавиатуры и мыши в ОС Windows 2000/XP/2003/2008/7. Используется драйвером ACRUN.SYS
	ACPROC.EXE	Программа для анализа журналов пользователей и составления списков процессов
	READPRD.EXE	Программа для просмотра файлов *.PRD
	ACCORD.SCR	Программа хранителя экрана Accord
	ACRUNVDD.EXE	Резидент для DOS-box, перенаправляющий файловые операции для анализа в драйвер ACRUN.SYS
	ACRUNVDD.DLL	Вспомогательная библиотека для ACRUNVDD.EXE

[5)] Драйвер состоит из двух драйверов: 1. работает по принципу TDI-фильтра и применяется в ОС Windows NT, Windows Server 2000, Windows XP, Windows Server 2003. 2. использует технологию Windows Filtering Platform и применяется в ОС Windows Vista и выше (находится в каталоге c:\accord.nt\Vista)

Функцио-нальное назначение программ	Наименование модуля	Назначение и краткая характеристика модуля
	ACSETUPTC.EXE	Программа для установки/снятия программной части системы защиты терминального клиента, а также изменения параметров ее функционирования
	USRTOAZ.DLL	Библиотека синхронизации баз пользователей accord.amz и АМДЗ. Используется программой ACED32.EXE
	AZIAHLP.DLL	Библиотека - интерфейс с базой пользователей в плате АМДЗ. Используется библиотекой USRTOAZ.DLL
	AMZTONT.DLL	Библиотека для синхронизации accord.amz и учетных записей Windows. Используется программой ACED32.EXE
	TMATTACH.DLL	Библиотека, которая содержит графическое представление работы с идентификатором. Используется программой ACED32.EXE
	TMDRV32.DLL	Библиотека для связи с драйвером контроллера АМДЗ. Используется библиотекой TMATTACH.DLL
	TMEXPLOR.EXE	Тестовая программа для проверки работоспособности платы АМДЗ под ОС Windows
	ACCORD.KEY	Файл лицензии для терминальной версии комплекса
	VCTMDRV.DLL	Библиотека для работы с виртуальными каналами. Используется при работе с терминальными клиентами
	ACRUNTI.EXE	Программа для вывода логотипа фирмы при работе терминального клиента
	CSTMDRV.DLL	Библиотека, реализующая виртуальный канал по протоколу ICA, на стороне сервера
	CWSTMDRV.DLL	Библиотека, реализующая виртуальный канал по протоколу ICA, на стороне клиента
	RDPTMDRV.DLL	Библиотека, реализующая виртуальный канал по протоколу RDP, на стороне сервера
	TMDRVRDP.DLL	Библиотека, реализующая виртуальный канал по протоколу RDP, на стороне клиента

7. Принцип работы комплекса

Плата контроллера «Аккорд-АМДЗ» из состава комплекса СЗИ НСД «Аккорд» устанавливается в свободный слот материнской платы СВТ. После регистрации администратора безопасности информации (супервизора) производится загрузка ОС, установка драйвера устройства и инсталляция специального программного обеспечения – подсистемы разграничения доступа в среде Windows на жесткий диск СВТ. Активизация монитора разграничения доступа, настройка комплекса, регистрация пользователей и установка правил разграничения доступа (ПРД) 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 и/или мандатного механизма разграничения – см. «Руководство администратора» (11443195.4012-037 90).

С помощью утилиты ACED32.EXE в специальный файл данных вносятся списки файлов, целостность которых будет проверяться при запуске СВТ данным пользователем. После регистрации пользователю выдается на руки персональный идентификатор, о чем делается запись в журнал учета носителей информации.

Особенностью и, несомненно, преимуществом комплексов АККОРД™ 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 комплекса. Внутреннее программное обеспечение контроллера, которое выполняет эти процедуры, защищено от модификации со стороны любого ПО, установленного на СВТ, т.к. хранится в области памяти, защищенной от записи.

Контроллер «Аккорд-АМДЗ» из состава комплекса СЗИ НСД «Аккорд-Win64» получает управление во время 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 «Аккорд-АМДЗ» при выполнении этой процедуры проводится идентификация/аутентификация пользователя и контроль целостности, а при ошибке возврат из процедуры не происходит, т.е. 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 4). Допускается установка длины пароля до 12 символов, по умолчанию длина пароля 8 символов.

При осуществлении контрольных процедур контроллер комплекса «Аккорд-АМДЗ» из состава комплекса «Аккорд» блокирует загрузку ОС с любых сменных носителей: флоппи-диска, CD-ROM и ZIP-drive, USB-disk и др.

После касания съемника информации Идентификатором 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.

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» на зеленом фоне 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 ОС не производится. Для продолжения работы потребуется вмешательство администратора БИ.

Все программное обеспечение, реализующее контрольные процедуры (идентификация, аутентификация, проверка целостности) хранится в энергонезависимой памяти контроллера комплекса «Аккорд-АМДЗ». Этим обеспечивается защита от разрушающих программных воздействий (РПВ) как встроенного ПО комплекса «Аккорд-АМДЗ», так и специального ПО разграничения доступа комплекса и ОС, размещаемых на жестком диске СВТ.

После старта ОС управление передается «ядру защиты» комплекса в составе модуля ACRUN.SYS – «монитора разграничения доступа» и модуля ACGINA.DLL – библиотеки динамической компоновки параметров доступа пользователей в Windows с учетом результатов их идентификации/аутентификации комплексом СЗИ НСД «Аккорд-АМДЗ».

Модуль ACRUN.SYS предназначен для разграничения доступа к ресурсам СВТ в соответствии с правилами разграничения доступа, назначенными администратором безопасности комплекса конкретному пользователю.

Модулем ACGINA.DLL осуществляется перехват стандартных запросов к MSGINA.DLL и их модификация для обеспечения работы комплекса «Аккорд-Win64». Библиотека ACGINA.DLL использует сведения о пользователе, который выполнил идентификацию/аутентификацию средствами контроллера комплекса «Аккорд-АМДЗ». На основании этих сведений разрешается вход в систему Windows зарегистрированных пользователей, и запрещается вход в систему неавторизованных пользователей. Сведения о пользователе, которому разрешен вход в систему, передаются модулю ACRUN.SYS.

Каждому пользователю, или группе пользователей администратор безопасности 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 – то есть выработанного непосредственно перед проверкой. Эталонный (контрольный) вектор вырабатывается на основе контрольной суммы защищаемых файлов и секретного ключа пользователя, который хранится в идентификаторе. Если предполагается санкционированная модификация защищенных файлов пользователем, то администратор может установить режим пересчета контрольных сумм при завершении сеанса работы пользователя.

Важной составляющей безопасности при работе ОС является динамический контроль целостности процессов (задач) в оперативной памяти СВТ. Администратор может задать список процессов для динамического контроля, и в процессе функционирования комплекса резидентная часть «монитора безопасности» 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 ОС и процесс запускается на исполнение. При отрицательном исходе проверки загрузка и запуск задачи не происходит.

Кроме того, «монитор разграничения доступа» ограничивает доступ пользователя к ресурсам, расположенным как локальных, так и на сетевых дисках, в соответствии с едиными правилами разграничения доступа (ПРД).

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

8. Поставка комплекса

Комплекс «Аккорд-Win64» v.5.0 (ТУ 4012-037-11443195-2010) поставляется в составе (базовая комплектация):

1) комплекс СЗИ НСД «Аккорд-АМДЗ» в комплекте[6]:

контроллер «Аккорд» -1 шт.;

съёмник информации (контактное устройство) - 1 шт;

персональный ТМ-идентификатор DS-199x – 2шт;

2) специальное ПО «Аккорд» версии 5.0 (разграничения доступа в среде Windows) – на CD;

3) внутреннее ПО контроллеров АМДЗ, драйверы платы, утилиты – на CD.

4) эксплуатационная документация - на CD;

5) формуляр на комплекс СЗИ НСД (11443195.4012-037 ФО) – 1 брошюра;

6) комплект упаковки.

[6] 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 информатизации (ОИ), осуществляется, как правило, специалистами по защите информации организации (предприятия, фирмы и т.д.) в соответствии с требованиями эксплуатационной документации на комплекс.

Установка комплекса «Аккорд» включает:

1) установку в СВТ аппаратной части комплекса – комплекса СЗИ НСД «Аккорд-АМДЗ», его настройку с учетом конфигурации технических и программных средств СВТ, в том числе, регистрацию администратора безопасности информации (или нескольких администраторов) и пользователей;

Установка и настройка комплекса СЗИ НСД «Аккорд-АМДЗ» осуществляется администратором БИ в соответствии с «Руководством по установке ПАК СЗИ НСД «Аккорд-АМДЗ» (11443195.4012-006 98) и «Руководством администратора» (11443195.4012-006 90).

2) установку на жесткий диск СВТ специального программного обеспечения разграничения доступа с дистрибутивных дискет (либо CD-ROM) и активизацию подсистемы разграничения доступа с помощью программы ACSETUP.EXE – осуществляется администратором БИ в соответствии с «Руководством по установке комплекса СЗИ НСД «Аккорд-Win64» (11443195.4012-037 98);

3) настройку защитных механизмов комплекса в соответствии с правилами разграничения доступа (ПРД) к информации, принятыми в организации (на предприятии, фирме и т.д.) – осуществляется администратором БИ в соответствии «Руководством администратора» (11443195.4012-037 90);

4) реализацию организационных мер защиты, рекомендованных в эксплуатационной документации на комплекс.

При использовании Системы удаленного централизованного управления средствами защиты информации от несанкционированного доступа «Аккорд» (СУЦУ СЗИ НСД «Аккорд») комплекс устанавливается также на сервер централизованного управления. В дальнейшем на сервере регистрируются в качестве подконтрольных объектов все СВТ с размещенным комплексом «Аккорд».

10. Управление защитой информации

Созданная структура защиты информации при применении комплекса «Аккорд» должна поддерживаться механизмом установления полномочий пользователей ПЭВМ (АС) и управлением их доступом к информационным ресурсам защищаемой АС.

Для этого на предприятии (учреждении, фирме и т.д.) должна создаваться служба безопасности информации (СБИ) или назначаться ответственное лицо (администратор безопасности информации), на которых возлагается разработка и ввод в действие организационно-правовых документов по применению СВТ с внедренными средствами защиты комплекса «Аккорд». Этими документами должно предусматриваться ведение ряда учетных и объектовых документов.

Перечень организационных мер, необходимых для обеспечения комплексом «Аккорд» требуемого уровня защиты информации, а также функции и обязанности администратора безопасности информации и пользователей приведены в «Руководстве администратора» (11443195.4012-037 90) и «Руководстве оператора (пользователя)» (11443195.4012-035 34), соответственно.

11. Правовые аспекты применения комплекса

Программно-аппаратные комплексы СЗИ НСД семейства «Аккорд»™ и сопутствующая документация защищены законом России об авторских правах, а также положениями Международного Договора. Любое использование комплексов 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 ПО, принадлежат ОКБ САПР (С), Россия, 115114, г. Москва, 2-й Кожевнический пер. д. 12. Предприятие-изготовитель разрешает делать архивные копии программного обеспечения комплексов семейства «Аккорд»™ 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 продукции АККОРД™ уведомление об авторских правах ни при каких обстоятельствах не допускается.

При необходимости применения комплексов «Аккорд»™ для других целей решение этого вопроса возможно только при наличии письменного согласия ОКБ САПР. Отметим, что предыдущие ограничения не запрещают вам распространять Ваши собственные исходные коды или модули, связанные с применением программного обеспечения комплексов «Аккорд»™. 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 комплексов «Аккорд»™, предприятие-изготовитель гарантирует их исправность в соответствии с гарантийными обязательствами, указанными в Формуляре.

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

Комплексы СЗИ НСД семейства «Аккорд»™ поставляются по принципу «as is», т.е. предприятие-изготовитель (ОКБ САПР) 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. Тем не менее, любые Ваши потери могут быть возмещены в том случае, если Вы оформите страховой полис по разделу «Страхование информационной безопасности». В этом случае возмещение возникшего ущерба будет обеспечено страховыми компаниями.

При покупке и применении комплексов СЗИ НСД «Аккорд»™ предполагается, что Вы знакомы с данными требованиями и согласны с положениями настоящего раздела.

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:

help@okbsapr.ru

support@okbsapr.ru

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

Приложение 1. Методические рекомендации по формированию и поддержке изолированной программной среды (ИПС)

Предположим, что в АС 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 безопасности информации (администратор БИ) АС, 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 СВТ 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 СВТ 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 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 программным 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 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 КС 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 течении 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.

предполагается, что в ПЗУ (BIOS) и операционной среде (в том числе и в сетевом ПО) 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:

5) Проверенные программы будут использованы на другом СВТ с другим BIOS и в этих условиях использоваться некорректно.

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

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

Тогда, НСД в АС гарантировано невозможен, если выполняются условия:

У1. На СВТ с проверенным BIOS установлена проверенная операционная среда.

У2. Достоверно установлена неизменность DOS 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 ослабляет требования к базовому ПО. 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 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 Условий 1-3, 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 разрушающее программное воздействие (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 данных. 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, что для обеспечения чтения реальных данных (защиты от РПВ) подсистема контроля целостности СЗИ НСД должна строиться на основе алгоритма ступенчатого (пошагового) контроля целостности.

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

При включении питания СВТ происходит тестирование ОП, инициализация таблицы прерываний и поиск расширений BIOS. При их наличии управление передается на них. После отработки расширений BIOS в память считывается первый сектор дискеты или винчестера (загрузчик) и управление передается на него, код загрузчика считывает драйверы DOS, далее выполняются файлы конфигурации, подгружается командный интерпретатор и выполняется файл автозапуска.

С учетом этого механизма для реализации ИПС предварительно фиксируется неизменность программ в основном и расширенных BIOS. Далее, используя 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.

Реализация ИПС с использованием механизма расширения BIOS

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 АС, который знает все Ki и единолично проводит этап установки. Пользователи же участвуют только в этапе эксплуатации.

Процесс установки ИПС состоит из следующих действий:

1) В СВТ 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 типа IBM PC для этой цели необходимо использовать механизм расширения BIOS.

2) Администратор 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.

3) Администратор 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.

4) Администратор проделывает действия 2 и 3 для всех N пользователей.

5) Администратор устанавливает в программную среду модуль активизации ИПС и фиксирует его целостность. Фиксируется также целостность файлов операционной среды Fос, в которые входят файлы DOS, драйверы и сетевое ПО.

Процесс эксплуатации состоит из следующих действий.

1) Включение питания и активизация расширенного BIOS:

идентификация пользователя по его Ki.

При успехе - п. б).

Проверка целостности всех включенных в ПЭВМ (PC) BIOS.

При положительном исходе - п. в).

Чтение файлов Fипс и Fос с помощью функций операционной среды и проверка их целостности.

При положительном исходе - п. г).

Активизация ОС и сетевого ПО.

Активизация процесса контроля Рипс.

Запуск избранной задачи i-го пользователя.

2) Работа в ИПС.

Запуск каждого процесса Ps сопровождается проверками:

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

Совпадает ли G=f(Ki,Fs,Ps) с M=f(Ki,Fs,Ps), вычисленной администратором БИ.

При положительном исходе проверки б) задача запускается.

Легко видеть, что условия изолированности среды (У1-5) в данном случае выполнены.

Пункт У1 гарантируется при установке системы администратором БИ.

Пункты У2, У4 и У5 обеспечиваются контроллером комплекса «Аккорд»™ (загрузка собственной ОС и сетевой среды с дискеты (других магнитных носителей) невозможна, поскольку расширенный BIOS активен раньше и направляет загрузку на жесткий диск; пользователь допускается к работе только при проверке Ki).

Пункт У3 реализован программным модулем контроля запусков и контроля целостности задач, входящим в состав ИПС. Кроме того, в данном случае реализован механизм ступенчатого контроля, обеспечивающий чтение реальных данных.

Приложение 2. Методика определения требуемой (целесообразной) длины пароля, используемого в комплексах СЗИ НСД семейства «Аккорд»™ 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 безопасности информации.

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. – 264 с.)

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

где

- k - количество попыток в минуту;
- 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 «Аккорд» - не менее 7 сек., т.е.

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

Для английского алфавита A=26 и S=7:

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

т.е. пароля длиной 7 символов достаточно для выполнения условия, а именно: Если будет выбран пароль длинной в 7 символов, то в течение 3-х месяцев вероятность подбора пароля будет не выше 0,001.

Если выбирается длина пароля в 6 символов (S=6), то выполняется неравенство:

$$3{,}7 * 10^{**}8 * M <= 3{,}089 * 10^{**}8,$$

или $M <= 0{,}83,$

т.е. при длине пароля 6 символов и регулярном тестировании в течении 25 дней вероятность подбора пароля составит не более 0,001.