ОКБ ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

УТВЕРЖДЕН
11443195.4012-026 90-ЛУ

Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «АККОРД-Х» (версия 1.0)

РУКОВОДСТВО АДМИНИСТРАТОРА

11443195.4012-026 90

Литера $О_1$

№ изменения	Подпись отв. лица	Дата внесения изм.

АННОТАЦИЯ

Настоящий документ является руководством по управлению механизмами защиты программно-аппаратного комплекса защиты информации от НСД «Аккорд-X» v.1.0 (ТУ 4012-026-11443195-2008) и предназначен для конкретизации задач и функций должностных лиц организации (предприятия, фирмы), планирующих и организующих защиту информации в системах и средствах информатизации на базе СВТ с применением комплекса.

В документе приведены основные функции администратора безопасности информации, порядок установки прав доступа пользователей к информационным ресурсам, организации контроля работы СВТ с внедренными средствами защиты и другие сведения необходимые для управления защитными механизмами комплекса.

Для лучшего понимания и использования защитных механизмов комплекса рекомендуется предварительно ознакомиться с комплектом эксплуатационной документации на комплекс, а также принять необходимые защитные организационные меры, рекомендуемые в документации.

Применение защитных мер комплекса должно дополняться общими мерами предосторожности и физической безопасности СВТ.

СОДЕРЖАНИЕ

Введение

Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «Аккорд-X» v.1.0 (ТУ 4012-026-11443195-2008), далее по тексту – комплекс «Аккорд», или ПАК СЗИ НСД «Аккорд» – это простой, но чрезвычайно эффективный комплекс технических и программных средств, используя который можно надежно защитить от несанкционированного доступа информацию на СВТ, функционирующих под управлением ОС Linux, без переделки ранее приобретенных программных средств.

Комплекс обеспечивает для пользователя «прозрачный» режим работы, при котором он, как правило, не замечает внедренной системы защиты. Таким образом, дополнительная нагрузка, связанная с эксплуатацией СЗИ НСД, не ложится на пользователя, а замыкается на администраторе безопасности информации (администраторе БИ). В этой связи для обеспечения эффективности работы СВТ администратор БИ обязан досконально изучить и правильно управлять применять возможностями системы защиты информации от НСД к информационным ресурсам АС, построенной на базе комплекса «Аккорд».

Комплекс СЗИ НСД «Аккорд-X» v.1.0. позволяет надежно обеспечить:

- защиту от несанкционированного доступа к АС (СВТ) и ее ресурсам;
- разграничение доступа к ресурсам СВТ, в т.ч. к внешним устройствам, управлением потоками информации в соответствии с уровнем полномочий пользователей, используя дискреционный и мандатный способы управления доступом пользователей к информационным ресурсам СВТ;
- защиту от несанкционированных модификаций программ и данных и различного рода проникающих разрушающих воздействий (ПРВ);
- контроль целостности конфигурации технических средств СВТ, программ и данных с реализацией пошагового алгоритма контроля целостности;
- создание изолированной программной среды (ИПС) с исключением возможности несанкционированного выхода в ОС, загрузки с FDD и несанкционированного прерывания контрольных процедур с клавиатуры;
- ввод широкого перечня дополнительных защитных механизмов в соответствии с политикой информационной безопасности, принятой в организации (на предприятии, фирме и т.д.).

Не умаляя достоинств комплекса, прежде всего сильной аппаратной поддержки большинства защитных механизмов, надо сказать, что комплекс не может решить все проблемы по созданию комплексной защиты информационных систем. Надо четко понимать, что комплекс «Аккорд» – это лишь хороший инструмент, позволяющий службе безопасности информации (администратору БИ) значительно проще и надежнее решать одну из стоящих перед ней задач – защиту от НСД к СВТ и информационным ресурсам АС, разграничение доступа к объектам доступа, обеспечение целостности программ и данных в соответствии с принятой в организации (предприятии, фирме и т.д.) политикой информационной безопасности.

Использование СВТ с внедренными средствами защиты комплекса не требует изменения существующего программного обеспечения. Необходимо лишь квалифицированное применение комплекса – правильная установка, настройка и эксплуатация в соответствии с принятыми на предприятии ПРД, и обеспечение организационной поддержки.

Как показывает практика довольно длительного применения комплексов СЗИ НСД семейства «Аккорд»™, часто трудности заключаются в отсутствии у большинства пользователей (организаций, фирм и т.д.) установленного порядка и четких правил разграничения доступа к защищаемым ресурсам. Поэтому, именно выяснение того, что и кому в СВТ доступно, а что нет, и какие действия с доступными ресурсами разрешено выполнять, а какие нет, является основным содержанием необходимой организационной поддержки.

Для выполнения этих задач, а также для обеспечения непрерывной организационной поддержки работы применяемых программно-технических средств защиты информации, в том числе и комплекса «Аккорд», необходима специальная служба безопасности информации (СБИ), в небольших организациях и подразделениях – администратор безопасности информации (администратор БИ). На СБИ (администратора БИ) возлагаются задачи по осуществлению единого руководства, организации применения средств защиты и управления ими, а также контроля за соблюдением всеми категориями пользователей требований по обеспечению безопасности информационных ресурсов автоматизированных систем. Правовой статус СБИ, обязанности и некоторые рекомендации по организации СБИ приведены в Приложении 1.

ВНИМАНИЕ!

Применение комплекса «Аккорд» совместно с сертифицированными программными СКЗИ и средствами разграничения доступа позволяет значительно снизить нагрузку на организационные меры, определяемые условиями применения этих средств. При этом класс защищенности не снижается.

Для эффективного применения ПАК СЗИ «Аккорд» и поддержания требуемого уровня защищенности СВТ необходимы:

- физическая охрана СВТ и ее средств, в т.ч. обеспечение мер по неизвлечению контроллера комплекса;
- использование в СВТ технических и программных средств, сертифицированных как в Системе ГОСТ Р, так и в системе Государственной системы безопасности информации (ГСЗИ);
- периодическое тестирование средств защиты комплекса;
- разработка и ведение учетной и объектовой документации (инструкция администратора, инструкций пользователей, журнал учета идентификаторов и отчуждаемых носителей пользователей и др.). Все разработанные учетные и объектовые документы должны быть согласованы, утверждены у руководства и доведены до сотрудников (пользователей). Это необходимо для того, чтобы План защиты организации (предприятия, фирмы и т.д.) и действия СБИ (администратора БИ) получили юридическую основу.
- прием в эксплуатацию ПАК СЗИ «Аккорд» оформляется актом в установленном порядке, в формуляре на комплекс администратором БИ делается соответствующая отметка.

1. СОДЕРЖАНИЕ РАБОТЫ АДМИНИСТРАТОРА БИ ПО ПРИМЕНЕНИЮ КОМПЛЕКСА

Основным содержанием работы администратора БИ по применению ПАК СЗИ «Аккорд» являются следующие мероприятия:

планирование применения комплекса;

организация установки комплекса и настройка его защитных средств в соответствии с установленными ПРД;

эксплуатация СВТ с внедренным комплексом, в т.ч., организация контроля за правильностью применения защитных механизмов комплекса;

снятие защиты.

1.1 Планирование применения комплекса

Планирование применения комплекса «Аккорд» осуществляется с учетом общей политики обеспечения безопасности в организации (на предприятии, фирме и т.д.). Основное содержание этой политики должно отражаться в Плане защиты организации (предприятия и т.д.) – документе, отражающем также подходы к защите информации и фиксирующем состояние защищаемой автоматизированной системы. В части защиты информации в него целесообразно включать сведения о характере и составе обрабатываемой информации, составе технических и программных средств АС (СВТ), возможных угрозах системе и наиболее вероятных способах их реализации, описание выбранных методов и средств защиты от этих угроз, правила разграничения доступа к информационным ресурсам и другие вопросы.

Для настройки средств защиты комплекса «Аккорд» в соответствии с разработанными и утвержденными в организации ПРД администратору БИ необходимо предварительно выяснить и отразить в плане защиты следующие характеристики защищаемой системы (СВТ):

- перечень задач, решаемых структурными подразделениями организации (сотрудниками) с использованием АС (СВТ);
- детальный перечень используемых при решении каждой задачи программ;
- детальный перечень используемых при решении каждой задачи (совместно используемых несколькими задачами) данных с указанием мест их размещения, режимов обработки и правил доступа к ним;
- конфигурацию СВТ с указанием перечня используемых технических средств (принтеров, сканеров и т.д.) и их характеристик;
- при использовании комплекса для защиты ЛВС – подробный перечень имеющихся в защищаемой сети серверов, рабочих станций и т.д. с указанием их состава, конфигурации, характеристик используемых технических средств и мест их размещения;
- перечень размещенных на СВТ (каждой рабочей станции ЛВС и каждом файловом сервере) системных и прикладных программ, файлов и баз данных;
- перечень установленных на СВТ (рабочих станциях и серверах) программных средств защиты (СКЗИ и СЗИ НСД);

- списки пользователей СВТ с указанием решаемых ими задач из общего перечня задач и предоставленных им (в соответствии с их обязанностями) полномочий по доступу в СВТ (рабочим станциям, серверам ЛВС) и информационным ресурсам.

На этапе организации системы защиты и применения комплекса «Аккорд» необходимо, исходя из целей защиты СВТ и ее специфики, разработать ряд документов, определяющих:

- порядок и правила предоставления, изменения и утверждения конкретным должностным лицом необходимых полномочий по доступу к ресурсам СВТ;
- порядок организации учета, выдачи, использования и хранения съемных магнитных носителей информации, содержащих резервные копии программ и данных и т.п.;
- порядок обновления используемых версий, приема в эксплуатацию новых системных и прикладных программ на защищаемых СВТ (рабочих станциях, серверах) – кто обладает правом разрешения таких действий, кто осуществляет, кто контролирует, и что при этом они должны делать – гарантирующий их безопасность и отсутствие РПВ;
- порядок использования, хранения и контроля целостности программных продуктов;
- порядок замены и ремонта средств вычислительной техники на защищаемой СВТ (в АС) – кто обладает правом разрешения таких действий, кто их осуществляет, кто контролирует, и что при этом они должны делать;
- порядок и периодичность анализа системных журналов регистрации и принятия мер по зарегистрированным несанкционированным действиям пользователей СВТ.

Для реализации впоследствии возможности создания любому пользователю изолированной программной среды (ИПС) необходимо, чтобы вышеназванные документы и правила разграничения доступа к ресурсам гарантировали:

- исключение возможности доступа непривилегированных пользователей к находящихся в СВТ инструментальным и технологическим программам, с помощью которых можно проанализировать работу СЗИ и предпринять попытки их «взлома» и обхода, внедрения разрушающих программных воздействий (РПВ);
- исключение возможности разработки программ в защищенном контуре СВТ (системы);
- исключение возможности несанкционированной модификации и внедрения несанкционированных программ;
- жесткое ограничение круга лиц, обладающими расширенными или неограниченными полномочиями по доступу к защищаемым ресурсам.

С учетом вышесказанного необходимо также разработать и внести необходимые изменения во все организационно-распорядительные документы (положения о подразделениях, функциональные обязанности сотрудников, инструкции пользователей и т.д.) по вопросам информационной безопасности и правилам работы на СВТ (в АС) с внедренными средствами защиты комплекса, действиям в случае возникновения нештатных ситуаций.

1.2 Установка и настройка комплекса

Администратор БИ организует установку комплекса «Аккорд», исходя из принятой в организации политики информационной безопасности и осуществляет контроль за качеством ее выполнения.

ВНИМАНИЕ!

Установка программных средств комплекса должна проводиться в присутствии администратора БИ.

В настоящем разделе рассматривается порядок настройки защитных механизмов комплекса в соответствии с правилами разграничения доступа (ПРД) к информации, принятыми в организации (на предприятии, фирме и т.д.).

Содержанием этой работы является назначение пользователям СВТ полномочий по доступу к ресурсам в соответствии с разработанными (и возможно уточненными в ходе настройки комплекса) организационно-распорядительными документами.

Полномочия пользователей по доступу к ресурсам АС (СВТ) назначаются с помощью программы ACX-ADMIN путем соответствующей настройки:

- средств идентификации и аутентификации пользователей, с учетом необходимой длины пароля и времени его жизни, ограничением времени доступа субъекта к СВТ;
- механизма управления доступом к ресурсам с использованием атрибутов доступа, которые устанавливаются администратором БИ в соответствие каждой паре «субъект доступа – объект доступа» при регистрации пользователей исходя из их функциональных обязанностей;
- средств контроля целостности критичных с точки зрения информационной безопасности программ и данных;
- механизма функционального замыкания программной среды пользователей средствами защиты комплекса;
- механизмов управления стандартными процедурами печати, процедурами ввода/вывода на отчуждаемые носители информации;
- дополнительных защитных механизмов, таких как блокирование экрана и клавиатуры в случаях, в которых могут реализовываться угрозы информации, а также подачи соответствующих звуковых и визуальных сигналов при попытках несанкционированного доступа к СВТ и ее ресурсам.

1.3 Эксплуатация комплекса

При эксплуатации комплекса администратор БИ решает следующие задачи:

- поддерживает средства защиты комплекса в работоспособном состоянии и контролирует правильность их работы;
- производит изменения в настройке средств защиты комплекса на основании и в полном соответствии с изменениями правил разграничения доступа. Они могут быть вызваны различными причинами, например, изменением состава пользователей, их должностных и функциональных обязанностей, расширением номенклатуры используемых технических и программных средств, задач и т.п.
- осуществляет текущий контроль за работой пользователей СВТ с внедренными средствами защиты комплекса;
- анализирует содержимое журнала регистрации событий, формируемого средствами комплекса и на этой основе вырабатывает предложения по совершенствованию защитных механизмов, реализуемых средствами комплекса, принимает необходимые меры по совершенствованию системы защиты информации в целом.

ВНИМАНИЕ!
Непрерывная организационная поддержка функционирования средств защиты комплекса предполагает обеспечение строгого соблюдения всеми пользователями требований СБИ (администратора БИ).

1.4 Снятие защиты

Снятие (отключение) средств защиты комплекса может потребоваться для установки на жесткий диск компьютера какого-либо нового программного обеспечения – операционной системы, прикладного ПО и т.д.

ВНИМАНИЕ!
Снятие защиты разрешено только администратору БИ (супервизору).

Для снятия защиты администратору БИ необходимо отключить подсистему разграничения доступа и снять аппаратную часть комплекса, для чего следует:

1. Загрузить СВТ и войти в систему с параметрами администратора БИ.

2. Запустить программу ACX-ADMIN из каталога /opt/accordx/. При этом запрашивается ТМ-идентификатор администратора БИ.

Если идентификация прошла успешно, то на экране появляется диалоговое окно, показанное на рис. 1.

3. В пункте меню «Команды» следует выбрать подпункт «Снятие» и выполнить действия, рекомендуемые программой. После выполнения команды «Снятие» подсистема разграничения доступа будет отключена, и при следующей загрузке не будет активизироваться. Каталог /opt/accordx остается на жестком диске. При необходимости можно полностью деинсталлировать ПО комплекса. Для этого необходимо в консоли выполнить команду «rpm –e accordx-admin».

4. Далее необходимо отключить питание СВТ.

5. Вскрыть корпус системного блока СВТ.

6. Извлечь аппаратную часть комплекса (контроллер).

2. ОСНОВНЫЕ МЕХАНИЗМЫ РЕАЛИЗАЦИИ ЗАЩИТНЫХ ФУНКЦИЙ КОМПЛЕКСА

Защитные механизмы комплекса «Аккорд» реализованы в соответствии с требованиями «РД. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», и «РД. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» Гостехкомиссия России, 1998. Реализация защитных функций выполнена в соответствии с требованиями по классу 1В для АС и 3-му классу для СВТ.

Ниже описаны защитные механизмы комплекса «Аккорд-Х» по схеме: «требование – реализация».

2.1. Требование идентификации и аутентификации

В соответствии с нормативными документами, комплекс средств защиты (КСЗ) должен требовать от пользователей идентифицировать себя при запросах на доступ. КСЗ должен подвергать проверке подлинность идентификатора субъекта – осуществлять аутентификацию. КСЗ должен располагать необходимыми данными для идентификации и аутентификации. КСЗ должен препятствовать доступу к защищаемым ресурсам не идентифицированных пользователей и пользователей, чья подлинность при аутентификации не подтвердилась. В требованиях к АС указывается минимальная длина пароля, которая должна составлять не менее 6 буквенно-цифровых символов.

Реализация

Реализация этих требований связана с выполнением условий создания изолированной программной среды (см. Описание применения. 11443195.4012-026 31), в том числе:

1. Идентификация должна выполняться трудно копируемым уникальным идентификатором до загрузки операционной системы.

2. Аутентификация должна выполняться с обеспечением защиты от раскрытия пароля – по крайней мере, пароль должен быть достаточной длины и проверяться он должен также до загрузки операционной системы (ОС).

3. Должен обеспечиваться контроль целостности программ и данных и на этой основе защита от несанкционированных модификаций программ и данных (с осуществлением основных контрольных функций до загрузки ОС).

4. В составе средств защиты от НСД должны быть средства, позволяющие обеспечить контроль запуска задач и на этой основе функциональное замыкание информационных систем с исключением возможности несанкционированного выхода в ОС.

Особенностью и, несомненно, преимуществом комплекса «Аккорд». является проведение на аппаратном уровне процедур идентификации и аутентификации до загрузки операционной системы. Это обеспечивается при помощи программного обеспечения, записанного в энергонезависимой флэш-памяти платы контроллера «Аккорд-АМДЗ» из состава комплекса «Аккорд».

Встроенное ПО «Аккорд-АМДЗ» из состава комплекса «Аккорд» получает управление на себя во время так называемой процедуры ROM-Scan, суть которой 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 2К. Признаком наличия ПЗУ является наличие слова AA55H в первом слове проверяемого интервала. Если данный признак обнаружен, то в следующем байте содержится длина ПЗУ в страницах по 512 байт. Затем вычисляется контрольная сумма всего ПЗУ, и если она корректна – будет произведен вызов процедуры, расположенной в ПЗУ со смещением 3. Такая процедура обычно используется для инициализации BIOS плат расширения. СЗИ «Аккорд» в этой процедуре проводит идентификацию и аутентификацию пользователя, контроль целостности аппаратной части СВТ, программ и данных. При любой ошибке возврат из процедуры не происходит, т.е. загрузка выполняться не будет.

Стойкость процедур идентификации и аутентификации определяется длиной пароля. Пример расчета требуемой длины пароля приведен в «Описании применения» (11443195.4012-026 31). Отметим, что в комплексе «Аккорд» используются и некоторые дополнительные механизмы защиты от НСД к компьютеру. Так, в частности, для пользователя администратор БИ может установить:

- время жизни пароля и его минимальную длину – например, исходя из расчетов, приведенных выше;
- временные ограничения – интервал времени по дням недели (с дискретностью 30 мин), в который разрешена загрузка СВТ данным пользователем (субъектом доступа);
- параметры управления экраном – гашение экрана через заранее определенный интервал времени (в случае, если в течение указанного интервала действия оператором не выполнялись);
- подача соответствующих звуковых и визуальных сигналов.

2.2. Требование гарантии проектирования

На начальном этапе проектирования КСЗ должна строиться модель защиты, задающая принцип разграничения доступа и механизм управления доступом. Эта модель должна содержать:

непротиворечивые правила изменения ПРД;

правила работы с устройствами ввода и вывода;

формальную модель механизма управления доступом.

Должна предлагаться высокоуровневая спецификация части КСЗ, реализующего механизм управления доступом и его интерфейсов. Эта спецификация должна быть верифицирована на соответствие заданных принципов разграничения доступа

Реализация

Описание попыток НСД в среде Linux

Попытки несанкционированного доступа могут быть проведены через:

1. *Операции файловой системы*

   К ним относятся попытки чтения, записи, модификации и т.д. файлов и каталогов локальной или сетевой СВТ. Отсутствие контроля над такими попытками позволяет неавторизованному пользователю получить доступ к любой информации находящейся в СВТ.

2. *Загрузка модулей и запуск программ.*

   Перехватив загрузку модулей можно отследить/запретить загрузку сторонних модулей (ELF, COFF, MISC, A.OUT, SO, KO) в системе, что позволяет избежать подмены системных модулей. Перехватив запуск исполняемых модулей, можно отследить/запретить запуск сторонних процессов в системе, что позволяет избежать запуска вредоносных программ.

Реализация разграничения доступа

Разграничение доступа к ресурсам СВТ в комплексе «Аккорд», (разграничение ресурсов – в терминах СЗИ НСД «Аккорд») реализовано при помощи резидентной программы, которая перехватывает на себя обработку функций дискового ввода/вывода. Смысл работы данного резидентного модуля в том, что при получении от пользовательской программы запроса, например, на удаление файла сначала производится проверка наличия таких полномочий у пользователя. Если такие полномочия есть – управление передается обычному обработчику ОС для исполнения операции. Если таких полномочий нет – имитируется выход с ошибкой.

2.3. Требование реализации дискреционного механизма разграничения доступа

КСЗ должен контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.).

Контроль доступа должен быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов).

Для каждой пары (субъект – объект) в СВТ должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т.д.), т.е. тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу СВТ (объекту).

Механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможности санкционированного изменения ПРД, в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов. Права изменять ПРД должны предоставляться выделенным субъектам (администрации, службе безопасности и т.д.). Должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ.

Реализация

Для реализации дискреционного механизма разграничения доступа необходимо по крайней мере конкретизировать термины, используемые в формальном описании. При этом целесообразно исходить из того, что полученная модель должна, с одной стороны, быть понятна пользователю, с другой – не ограничивать пользователя в реализации процедур разграничения доступа и как можно ближе соответствовать особенностям архитектуры технических средств компьютера и особенностям операционной системы. С этой точки зрения необходимо определить, что

целесообразно выбрать в качестве объектов разграничения доступа, и какие допустимые типы доступа целесообразно использовать.

Обсуждая этот вопрос, отметим, что в качестве объектов в большинстве ОС используются: Диски – каталоги (папки) – файлы (задачи).

Выбор типов доступа целесообразно связать с функциями ОС, посредством которых осуществляется доступ к ресурсам. Перехват вызовов этих функций позволит реализовать ПРД для явных действий пользователя.

Реализация ПРД для скрытых действий пользователя может быть осуществлена за счет ограничения перечня задач, которые пользователь имеет право запускать. Это означает, что средства ПРД должны содержать возможность явного и недвусмысленного описания перечня задач, запуск которых разрешен пользователю, и средств контроля за использованием этих задач. Формирование перечня должно осуществляться администратором БИ в порядке, предусмотренном для формирования и изменения ПРД.

В комплекс «Аккорд» дискреционные правила разграничения доступа устанавливаются присвоением объектам доступа атрибутов доступа. Установленный атрибут означает, что определяемая атрибутом операция может выполняться над данным объектом. В комплексе применяются следующие атрибуты:

R – открытие файлов для чтения;

W – открытие файлов для записи;

O – подмена атрибута R атрибутами RW на этапе открытия файла;

C – создание файлов;

D – удаление файлов;

N – переименование файлов и подкаталогов;

V – видимость файлов;

M – создание каталогов;

E – удаление каталогов;

n – переименование каталогов;

G – доступность данного каталога (т.е. переход к нему);

X – исполнение задач;

S – наследование подкаталогами атрибутов родительского каталога;

Установленные атрибуты определяют важнейшую часть ПРД пользователя. От правильности выбора и установки атрибутов во многом зависит эффективность работы СЗИ. В этой связи администратор службы безопасности информации должен ясно представлять, от чего и как зависит выбор атрибутов, назначаемых объектам, к которым имеет доступ пользователь. Как минимум, необходимо изучить принцип разграничения доступа с помощью данных атрибутов, а также особенности работы программных средств, которые будут применяться пользователем при работе.

Специальная программа – редактор прав доступа, позволяет администратору БИ для каждой пары субъект – объект определить:

Для дисков:

- доступность, т.е. пользователю доступны только те логические диски, которые явно описаны в ПРД;

Для каталога:

- доступность (переход к данному каталогу);
- видимость (данный каталог будет виден пользователю);
- наследование подкаталогами атрибутов каталога;

Для содержимого каталога:

- создание подкаталогов;
- удаление подкаталогов;
- переименование подкаталогов;
- открытие файлов для записи;
- открытие файлов для чтения;
- создание файлов;
- переименование файлов;
- удаление файлов;
- видимость файлов;
- «фиктивное» открытие файлов для записи;

Для задач:

- исполнение;

Дополнительно могут определяться Права доступа к отдельным файлам (с указанием полного пути доступа) – эти права будут обеспечиваться в безусловном порядке, даже если файл расположен в каталоге, доступа к которому данный пользователь не имеет, или атрибуты доступа для файла отличны от атрибутов каталога, в котором он находится. Предусмотрено определение следующих прав:

- открытие файлов для записи;
- открытие файлов для чтения;
- создание файлов;
- удаление файлов;
- переименование файлов;
- видимость файлов;
- «фиктивное» открытие файлов для записи;
- запуск задач.

Существует также и «черный список». Это файлы, или каталоги, которые присутствуют в списке объектов, для которых не установлен **ни один** атрибут доступа. Объекты, описанные в «черном списке», становятся недоступными пользователю, даже если они расположены в каталогах, к которым пользователь имеет доступ. В «черный список» можно включать также логические имена устройств и драйверы устройств. Эти объекты после такого описания становятся недоступны пользователю. Таким образом, осуществляется сопоставление пользователя и доступных ему устройств.

Кроме этого, в подсистеме дискреционного доступа реализованы два дополнительных атрибута, предназначенных для регистрации обращения пользователя к отдельным ресурсам. Атрибут «r» – определяет регистрацию операций чтения для отдельного объекта, атрибут «w» – регистрацию операций записи.

Использование этих атрибутов целесообразно в случае, когда администратору безопасности необходимо иметь информацию обо всех случаях обращения (даже санкционированным) к критичным ресурсам, а не только сообщения об НСД.

2.4. Требование по реализации мандатного принципа контроля доступа

Для реализации этого принципа должны сопоставляться классификационные метки каждого субъекта и каждого объекта, отражающие их место в соответствующей иерархии. Посредством этих меток субъектам и объектам должны назначаться классификационные уровни (уровни уязвимости, категории секретности и т.п.), являющиеся комбинациями иерархических и неиерархических категорий. Данные метки должны служить основой мандатного принципа разграничения доступа.

КСЗ при вводе новых данных в систему должен запрашивать и получать от санкционированного пользователя классификационные метки этих данных. При санкционированном занесении в список пользователей нового субъекта должно осуществляться сопоставление ему классификационных меток. Внешние классификационные метки (субъектов, объектов) должны точно соответствовать внутренним меткам (внутри КСЗ).

КСЗ должен реализовывать мандатный принцип контроля доступа применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов:

- субъект может читать объект, только если иерархическая классификация в классификационном уровне субъекта не меньше, чем иерархическая классификация в классификационном уровне объекта, и неиерархические категории в классификационном уровне субъекта включают в себя все иерархические категории в классификационном уровне объекта;

- субъект осуществляет запись в объект, только если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации, и все иерархические категории в классификационном уровне субъекта включаются в неиерархические категории в классификационном уровне объекта.

Реализация мандатных ПРД должна предусматривать возможности сопровождения: изменения классификационных уровней субъектов и объектов специально выделенными субъектами.

В КСЗ должен быть реализован диспетчер доступа, т.е. средство, осуществляющее перехват всех обращений субъектов к объектам, а также разграничение доступа в соответствии с заданным принципом разграничения доступа. При этом решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его и дискреционными, и мандатными ПРД. Таким образом, должен контролироваться не только единичный акт доступа, но и потоки информации.

Реализация

Разграничение доступа с использованием мандатного механизма управления доступом комплекса «Аккорд» осуществляется путем присвоения (задания) объектам доступа категории доступа (грифа), которые характеризуются уровнем доступа от 0 (самый низкий) до 15 (максимальный). Установленный для объекта доступа гриф является его меткой конфиденциальности.

Пользователям и процессам (опционально) присваиваются категории доступа (уровни допуска), также изменяющиеся от 0 до 15. Доступ пользователя или процесса возможен тогда и только тогда, когда его уровень допуска не ниже грифа объекта доступа.

Категории доступа могут быть поименованы как уровни секретности, либо другим, более удобным для Администратора БИ образом.

По умолчанию в комплексе определены 5 категорий конфиденциальности (секретности):

Level0=Общедоступно

Level1=Для бухгалтерии

Level2=Конфиденциально

Level3=Секретно

Level4=Совершенно секретно

Администратор БИ имеет право изменять названия и количество категорий конфиденциальности – но не более 15-ти. С увеличением номера категории повышается конфиденциальность данных. Далее необходимо установить уровень допуска пользователей. Это делается с помощью программы ACX-ADMIN – пункт меню «Команды», далее «Уровень доступа». После этого Администратор БИ может назначать как для каталогов, так и для отдельных файлов требуемые уровни доступа.

Проверка прав доступа субъекта (пользователя или процесса) к какому либо объекту доступа (ресурсу СВТ, либо АС) осуществляется в следующем порядке:

1. Проверяется, имеет ли пользователь права на доступ, установленные дискреционным механизмом комплекса.
2. Если пользователю установлены права по доступу дискреционным механизмом комплекса, то проверяется уровень допуска пользователя и гриф (метка конфиденциальности) объекта доступа (ресурса СВТ, либо АС).
3. Доступ будет разрешён только в том случае, если уровень допуска пользователя больше, либо равен грифу (метке конфиденциальности) объекта доступа (ресурса СВТ, либо АС).

В комплексе «Аккорд» реализована дополнительная функция, позволяющая устанавливать уровень доступа исполняемому процессу, когда он загружается в оперативную память. Исполняемому файлу (программе) присваивается метка конфиденциальности (уровень доступа) как объекту на диске СВТ. При этом файл (программа) будет запускаться только пользователем с определённым уровнем допуска.

После успешной загрузки в оперативную память исполняемый файл (программа), получает метку уровня доступа как субъект доступа, который работает с объектами (ресурсами). В этом случае проверка доступа к ресурсу осуществляется в следующем порядке:

1. Проверяется, имеет ли пользователь право на доступ в соответствии с дискреционным механизмом.
2. При наличии дискреционных прав доступа пользователя средствами мандатного механизма комплекса проверяется уровень его допуска и гриф (метка конфиденциальности) объекта доступа (ресурса).
3. Если доступ разрешён, то проверяется, имеет ли текущий процесс уровень допуска больше либо он равен уровню доступа объекта (ресурса), к которому обратился пользователь с помощью этого процесса.

4. Доступ будет разрешен только в случае успешного выполнения трёх вышеописанных проверок.

При такой реализации механизма управления потоками информации, обработка информации определённого уровня конфиденциальности выполняется только с помощью выделенных программ (процессов).

2.4. Требование управления потоками информации

Должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

Реализация

В комплексе «Аккорд» реализован механизм управления потоками информации, основанный на принципах мандатного разграничения доступом (см. выше п. 2.3.). При такой реализации механизма управления потоками информации, обработка информации определённого уровня конфиденциальности выполняется только с помощью выделенных программ (процессов).

Как для каталогов, так и для отдельных файлов может быть установлена метка конфиденциальности, а каждому пользователю присваивается метка уровня доступа. Если механизм мандатного доступа включен, то пользователь получит доступ только к тем объектам, метка конфиденциальности которых не выше уровня доступа субъекта (пользователя).

В комплексе реализована дополнительная функция, которая позволяет установить уровень доступа процессу в оперативной памяти. Таким образом, исполняемый файл (программа) имеет метку конфиденциальности, как объект на диске СВТ и может запускаться только пользователем с определенным уровнем доступа, а после загрузки в оперативную память получает метку уровня доступа, как субъект, который работает с объектами, имеющими соответствующую метку конфиденциальности. При такой реализации механизма управления потоками информации обработка информации определенного уровня конфиденциальности выполняется только с помощью выделенных программ (процессов). При этом процессу автоматически присваиваются атрибуты доступа, которые запрещают запись информации на носитель, метка конфиденциальности которого ниже уровня доступа процесса.

2.5. Требование регистрации событий

КСЗ должен быть в состоянии осуществлять регистрацию следующих событий:

- использование идентификационного и аутентификационного механизма;
- запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.);
- создание и уничтожение объекта;
- действия по изменению ПРД.

Для каждого из этих событий должна регистрироваться следующая информация:

- дата и время;
- субъект, осуществляющий регистрируемое действие;
- тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа);

- успешно ли осуществилось событие (обслужен запрос на доступ или нет).

КСЗ должен содержать средства выборочного ознакомления с регистрационной информацией, а также регистрировать все попытки доступа и действия выделенных пользователей (администраторов защиты и т.п.).

Обсуждение

Представляется нецелесообразным постоянно осуществлять полномасштабную регистрацию всех попыток доступа всех пользователей ко всем ресурсам – в первую очередь, из-за высоких накладных расходов. В то же время, вполне представимы ситуации, при которых необходима полная трассировка событий. В частности, именно такой способ следует применять, изучая, какие ресурсы требует новая программа – перед тем, как передать ее для эксплуатации пользователям. В этой связи целесообразно выделить несколько уровней детальности журнала. Установку уровня детальности для пользователя следует поручить администратору БИ в порядке, предусмотренном для установки и изменения ПРД.

Реализация

Как для каталогов, так и для отдельных файлов может быть установлена опция регистрации доступа к каталогу и его содержимому в регистрационном журнале. Регистрация осуществляется в следующем порядке:

- для каждого пользователя администратор БИ устанавливает уровень детальности журнала – низкая, средняя, высокая;
- для любого уровня детальности в журнале отражаются параметры регистрации пользователя, доступ к устройствам, запуск задач, попытки нарушения ПРД, изменения ПРД (в частности, изменение паролей);
- для среднего уровня детальности в журнале отражаются дополнительно все попытки доступа к защищаемым дискам, каталогам и отдельным файлам, а также попытки изменения некоторых системных параметров – даты, времени и др.;
- для высокого уровня детальности в журнале отражаются дополнительно все попытки доступа к содержимому защищаемых каталогов.

Кроме этого, предусмотрен механизм принудительной регистрации доступа к объектам. Для этого введены два дополнительных атрибута, а именно:

r – фиксировать в журнале все попытки доступа к объекту на чтение;

w – фиксировать в журнале все попытки доступа к объекту на запись.

Используя эти атрибуты, администратор может обеспечить регистрацию событий, важных для поддержания необходимого уровня информационной безопасности.

Программа ACX-ADMIN позволяет осуществить просмотр, вывод на печать и архивацию журнала регистрации событий комплекса защиты от НСД «Аккорд». Журнал отображается в виде таблицы. Каждая строка таблицы соответствует одному событию, зарегистрированному в журнале.

Журнал содержит следующую информацию:

- дата и точное время регистрации события;
- детальность журнала, установленная на момент регистрации события;
- имя рабочей станции;
- тип операции – в таблице выводится краткая аббревиатура;

- объект доступа – в таблице выводится полное наименование объекта доступа. Объектом доступа может быть файл, каталог, диск, устройство. Если событием является изменение прав доступа – в этом поле отображаются обновленные Права доступа.
- Результат события. При положительном завершении события результат – «ОК», при отрицательном – регистрируется несанкционированный доступ (НСД) или ошибка доступа (в случае нарушения целостности сообщается об изменении параметров контроля).
- Имя Процесса – программа, осуществляющая доступ к объекту в момент регистрации события. Для удобства просмотра и анализа информации можно выполнять фильтрацию по одному или нескольким полям таблицы. В Приложении 2 приведен справочник, который содержит как краткое, так и полное наименование операций, регистрируемых подсистемой регистрации.

2.6. Требование целостности комплекса средств защиты (КСЗ)

В СВТ должны быть предусмотрены средства периодического контроля за целостностью программной и информационной части КСЗ. Программы КСЗ должны выполняться в отдельной части оперативной памяти.

Обсуждение

Обычно для контроля целостности используется вычисление контрольной суммы. Вычисленное значение сравнивается с эталонным, и результат сравнения позволяет судить о состоянии программ и данных – остались ли они неизменными, были ли несанкционированные модификации. Казалось бы – все нормально, но вот беда – как убедиться в целостности процедур контроля? Ведь можно модифицировать и процедуру расчета контрольных сумм, и процедуру контроля процедуры расчета контрольных сумм и т.д. Кажется, что выхода из этого круга нет – невозможно обеспечить целостность программных средств за счет других программных средств, как невозможно вытащить самого себя за волосы из болота (но попытки были, а в области информационной безопасности они продолжаются и до сих пор). С этой неясностью можно покончить только одним способом – вынести процедуры контроля за пределы компьютера, т.е. выполнять их аппаратно (или с использованием аппаратных средств).

Еще одна проблема – это качество самих процедур контроля. Рассмотрим следующий случай – для контроля применяется контрольная сумма, вычисляемая по алгоритму CRC (именно так обычно и происходит). Для наглядности предположим, что используется CRC-3 (реально, естественно, используется от CRC-8 до CRC-32, но усложнение при этом носит чисто технический характер). Для CRC-3 количество значений – 8 (от 0 до 7). Допустим, контрольная сумма исходного (правильного) набора документов C1=3. К этому пакету злоумышленник добавляет еще несколько, таких, что их контрольная сумма C2=2. Таким образом, контрольная сумма модифицированного пакета документов Cm=(C1 + C2)mod8 = 5. Теперь для того, чтобы эта модификация не была обнаружена, злоумышленник вполне может к уже модифицированному пакету добавить еще несколько документов, таких, что их контрольная сумма C3=6. Контрольная сумма модифицированного пакета становится Cm=(C1 + C2 + C3)mod8 = (3 + 2 + 6)mod8 = 3, т.е. Cm = C1, и модификация не будет замечена контрольными процедурами. В общем случае, достаточно подобрать такой пакет, для которого (C2 + C3)mod8 = 0, и информационная атака может быть успешной. Общий источник возможности таких атак состоит в том, что значения применяемых алгоритмов вычисления контрольных сумм распределены равномерно (или просто известным образом). Соответственно, хорошей защитой может служить применение алгоритмов с существенно нелинейным распределением значений.

Реализация

Контроль целостности в комплексе «Аккорд» выполняется следующим образом.

Целостность самой контрольной процедуры обеспечивается тем, что хранится она не на диске, а в ЭНП контроллера комплекса СЗИ НСД «Аккорд-АМДЗ», будучи тем самым защищена от модификаций. При нормальном осуществлении процедур защиты от НСД (идентификации и аутентификации) копия контрольных процедур помещается в специально отведенную область ОЗУ и затем запускается на исполнение. Интерес представляет и следующий вопрос. В реальных условиях необходимо контролировать целостность многих файлов. Естественно, что хранить эталонные значения контрольных сумм для всех них на внешнем носителе с ограниченным объемом памяти невозможно.

В комплексе «Аккорд» применяется следующий механизм:

1. Контроль целостности системных областей диска, файлов ОС и прикладного ПО осуществляется на аппаратном уровне контроллером «Аккорд АМДЗ» до загрузки ОС.

2. Если процедура контроля из п. 1 выполнена успешно, то в момент запуска подсистемы разграничения доступа может выполняться контроль целостности файлов, по индивидуальному списку каждого пользователя. На диске хранится файл, содержащий перечень контролируемых файлов и эталонные значения контрольных сумм. По этим данным определяется целостность каждого конкретного файла.

3. Целостность же самого этого файла на диске обеспечивается тем, что эталонное значение его контрольной суммы вычисляется с использованием ключа, который хранится в идентификаторе пользователя. Этот ключ генерируется при регистрации идентификатора с использованием датчика случайных чисел, установленного на плате контроллера, и для каждого пользователя является уникальным.

В комплексе «Аккорд» предусмотрен динамический контроль целостности исполняемых модулей (задач). Этот контроль выполняется при каждом запуске модуля, независимо от того, выполняется ли эта операция пользователем, или ОС. При несовпадении вычисленной КС с эталонным значением блокируется запуск такого модуля.

Дополнительно в комплексе предусмотрен динамический контроль целостности собственно монитора разграничения доступа. Этот контроль выполняется периодически и обеспечивает дополнительный уровень защиты от случайных или преднамеренных покушений на отключение СЗИ.

В разделе 2.13. «Требования к классу защищенности 1В» Руководящего документа Гостехкомиссии России, 1998 – «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» приведено требование о тестировании функций СЗИ НСД, а именно: «должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в год».

Порядок такого тестирования определяется планом защиты и выполняется с помощью специализированных программных средств непосредственно на технических средствах АС. Тем не менее, есть один принципиально важный элемент СЗИ НСД, тестирование которого следует осуществлять на специализированных рабочих местах. Таким элементом являются программы системной BIOS и расширений BIOS.

Действительно, как было показано выше, надежная защита от НСД обеспечивается созданием изолированной программной среды (ИПС), причем поддержание ИПС возможно только при использовании пошагового алгоритма

контроля целостности, который, в свою очередь, отталкивается от некоторого начального состояния системы, при котором целостность используемых на данном этапе компонент зафиксирована.

Для СВТ типа IBM PC на первом этапе загрузки исполняется программа системного BIOS. Именно эта программа определяет процедуры чтения реальных данных для следующего этапа. Таким образом, использовать процедуры чтения, загруженные из ПЗУ BIOS, для контроля целостности самого BIOS было бы абсолютно некорректно, и создавало бы возможность для внедрения РПВ.

Тем не менее, целостность программных средств BIOS необходимо обеспечить. В данных условиях это требование следует выполнять за счет применения организационных мер и периодически выполняемого тестирования. При этом тестирование и проверка целостности BIOS должна осуществляться на специальных стендах со специальным программным обеспечением. Такой стенд может быть включен в состав АС, либо может находиться в специализированной организации, которая выполняла бы функции контроля по договору с организацией, эксплуатирующей АС на основании лицензии Гостехкомиссии России.

2.7. Требование очистки памяти.

При первоначальном назначении или при перераспределении внешней памяти КСЗ должен предотвращать доступ субъекту к остаточной информации. КСЗ должен осуществлять очистку оперативной и внешней памяти. Очистка должна производиться путем записи маскирующей информации в память при ее освобождении (перераспределении).

Обсуждение

Если с внешней памятью все ясно, то с оперативной есть проблемы. В частности – средствами DOS блок памяти выделяется задаче, и сама задача своими средствами может захватывать блоки памяти. При реализации функций очистки памяти важно очищать как то, так и другое.

Реализация

В комплексе «Аккорд» осуществляется перехват функций освобождения памяти и завершения задачи. Именно при этом и выполняется очистка оперативной памяти (освобождаемого блока). Очистка внешней памяти на диске выполняется опционно.

Соответствующая опция «**Число проходов при удалении» –** количество проходов случайной последовательности по содержимому файла на диске при его удалении, устанавливается администратором БИ при создании ПРД пользователя.

Опционный механизм применен в связи с тем, что очистка внешней памяти требует определенных временных затрат, которые не всегда (исходя из значимости защищаемых ресурсов) оправданы.

Атрибуты устанавливаются с помощью редактора ПРД к СВТ и информационным ресурсам АС.

3 НЕКОТОРЫЕ ОСОБЕННОСТИ ДЕЙСТВИЯ АТРИБУТОВ И ПОДГОТОВКИ ПРД

Часто перед нормальной попыткой открыть существующий файл программы выполняют просмотр содержимого каталога. В этом случае, если атрибут «V» не установлен, функции FindFirst и FindNext возвратят результат «ошибка». В некоторых случаях (при некорректной установке атрибутов) это может быть источником коллизий.

Отметим, что все атрибуты, кроме атрибута «G», относятся к содержимому каталога. Атрибут «G» относится к собственно каталогу.

Отдельно стоит рассмотреть применение атрибута «O». Введение этого атрибута связано с тем, что ряд программ открывают файл на чтение и запись, хотя реально используют только операции чтения. В этом случае пользователю приходится разрешать Права доступа и на чтение, и на запись, что потенциально может служить источником информационных угроз. Чтобы избавиться от этой опасности, можно «разнести» данные по специальным каталогам. Это вполне возможный путь, однако, его применение приводит к усложнению «Плана защиты» и увеличению количества каталогов. Введенный в СЗИ «Аккорд» атрибут «O» позволяет решить задачу другим методом, а именно: атрибут «O» подменяет (для задачи) атрибут «R» на совокупность атрибутов «R» и «W». При этом операция открытия файла проходит нормально, а попытка записи в этот файл классифицируется как НСД. Решение о применении для описания ПРД пользователей атрибута «O» принимается администратором БИ в том случае, когда файл по плану защиты должен быть доступен пользователю только для чтения, а применяемая для обработки данных программа пытается открыть этот файл и на чтение, и на запись. Анализ ситуации может быть выполнен путем изучения журнала при тестировании программного обеспечения, планируемого для включения в состав программных средств АС.

Обратите внимание на доставку информации в виде исполняемого файла – не важно, в каком виде осуществляется доставка – по сети, с помощью отчуждаемого носителя и др. Для того чтобы избежать неприятностей, нужно запрещать запуск задач из всех каталогов, кроме тех, в которых хранятся проверенные модули. Следует также обратить внимание на использование отчуждаемых носителей – как в плане разрешения на использование (далеко не каждому пользователю это необходимо), так и в плане регистрации и учета.

4 ПРАВОВЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ КОМПЛЕКСА

Программно-аппаратный комплекс СЗИ НСД «Аккорд-X» v.1.0 и сопутствующая документация защищены законом России об авторских правах, а также положениями Международного Договора. Любое использование данного комплекса в нарушение закона об авторских правах или в нарушение положений ЭД на комплекс будет преследоваться ОКБ САПР в силу наших возможностей.

Авторские права на данное изделие, в том числе аппаратные средства и специальное ПО, принадлежат ОКБ САПР, Россия, 115114, г. Москва, 2-й Кожевнический пер. д.8, тел. (499) 235-29-90, 235-62-65, факс: (495) 234-03-10, E-mail: okbsapr@okbsapr.ru.

ОКБ САПР разрешает Вам делать архивные копии программного обеспечения комплекса АККОРД™ для использования потребителем, приобретшим комплекс АККОРД™ в установленном порядке. Ни при каких обстоятельствах программное обеспечение комплекса АККОРД™ не распространяется между другими предприятиями (фирмами) и лицами.

Удалять в продукции комплекса АККОРД™ уведомление об авторских правах ни при каких обстоятельствах не допускается.

Применение средств комплекса АККОРД для других целей 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 комплекса 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.

ОКБ САПР гарантирует исправность физических экземпляров аппаратуры и документации, поставляемых в составе комплекса АККОРД, согласно формуляру на этот комплекс.

Мы просим пользователя при обнаружении ошибок или дефектов направить нам подробный отчет о возникших проблемах, который позволит найти и зафиксировать проблему.

Комплекс АККОРД поставляется по принципу «as is», т.е. 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 АККОРД. Тем не менее, любые Ваши потери могут быть возмещены в том случае, если Вы оформите страховой полис по разделу «Страхование информационной безопасности». Страховка оформляется по Вашему требованию непосредственно у поставщика.

При покупке и применении комплекса АККОРД предполагается, что Вы знакомы с данными требованиями авторов разработки и изготовления комплекса АККОРД и согласны с положениями настоящего раздела.

ОКБ САПР предлагает телефонную поддержку при технической возможности без дополнительной оплаты. Звоните нам по телефонам поддержки (499) 235-89-17, (926) 235-89-17 с понедельника по пятницу с 11-00 до 18-00 (по московскому времени), по существу вопросов о применении комплекса АККОРД. ОКБ САПР использует для поддержки связи с пользователями адрес SUPPORT@OKBSAPR.RU. Нам удобнее принимать и обрабатывать Ваши сообщения именно таким образом.

5 Приложения

Приложение 1.

Рекомендации по организации службы информационной безопасности

Ответственными за защиту информации в АС (СВТ) являются все руководители и отдельные пользователи (операторы) в пределах их служебной компетенции.

Для непосредственной организации и обеспечения функционирования системы защиты информации, как компонента АС, в организации (на предприятии, фирме – далее по тексту организации) должны быть предусмотрены специальные органы или ответственные лица – служба безопасности информации (СБИ) или администратор безопасности информации.

Сотрудники СБИ (администратор БИ) помимо безупречной репутации и полного доверия со стороны руководства организации должны обладать определенным уровнем знаний и навыков в области вычислительной техники, достаточным для ясного понимания всех видов угроз аппаратным и программно-информационным ресурсам АС (СВТ) и необходимым для грамотного управления и эффективного применения средств защиты.

Организационно-правовой статус СБИ (администратора БИ).

СБИ (администратор БИ) должны подчиняться тому лицу, которое в данной организации несет персональную ответственность за соблюдение правил обращения с защищаемой информацией;

сотрудники службы (администратор БИ) должны иметь право доступа во все помещения, где установлена аппаратура АС и право прекращать автоматизированную обработку информации при наличии или угрозе утечки защищаемой информации;

руководителю СБИ (администратору БИ) должно быть предоставлено право запрещать включение в число действующих новые элементы компонентов АС, если они не отвечают требованиям защиты информации;

службе БИ (администратору БИ) должны обеспечиваться все условия, необходимые для выполнения своих функциональных обязанностей;

численность службы должен быть достаточным для выполнения перечисленных выше функций, при этом штатный состав не должен иметь (по возможности) других обязанностей, связанных с функционированием АС.

Создаваемая структура защиты информации в СВТ при применении комплексов СЗИ НСД «Аккорд»™ должна поддерживаться механизмом установления полномочий пользователям СВТ и управлением их доступом к информационным ресурсам. Для этого СБИ (администратор БИ) разрабатывает и вводит в действие установленным в организации порядком организационно-правовые документы по применению СВТ с внедренными средствами защиты с учетом действующих нормативных и законодательных документов.

Обязанности администратора БИ по применению комплексов СЗИ НСД АККОРД™:

1. На основе «Плана защиты», введенного в организации, разрабатывать таблицы разграничения доступа к защищаемым ресурсам, вводить (при установке комплекса) полномочия пользователей и корректировать их в ходе эксплуатации СВТ.

2. Устанавливать комплекс защиты в СВТ и организовывать ее эксплуатацию с внедренными средствами защиты.

ВНИМАНИЕ!

После установки комплекса в СВТ должны быть приняты меры по обеспечению неизвлечения платы контроллера (опечатывание мастичной печатью, покрытой силикатным клеем (жидким стеклом) или др.

3. Тщательно анализировать процессы функционирования программ, которые будут закреплены за пользователями, в соответствии с этим создавать для каждого из них изолированную программную среду исполнения задачи, исходя из их функциональных обязанностей.

ВНИМАНИЕ!

Нежелательно, чтобы программы, закрепленные за пользователями, имели возможность доступа к дискам по абсолютным секторам, возможность прямого редактирования памяти.

4. Обучать пользователей правилам обработки защищаемой информации, контролировать правильность применения ими средств защиты комплекса и оказывать помощь в части организации работы на СВТ с внедренным комплексом защиты.

5. Контролировать на целостность (на уровне контроллера) файлы СПО разграничения доступа.

6. Выявлять возможные каналы НСД к информации при применении комплекса, готовить предложения по их устранению.

7. Систематически анализировать состояние комплекса и его отдельных средств, периодически проводить их тестирование и проверку защитных функций комплекса, о чем делать отметку в формуляре.

8. Регулярно анализировать содержание системного журнала и разрабатывать меры по исключению неправильного применения комплекса пользователями.

ВНИМАНИЕ!

Администратор должен довести до пользователей распоряжение о запрете снятия задач с выполнения при помощи выключения питания или нажатия на клавишу <RESET>.

9. Разрабатывать и вводить установленным порядком необходимую учетную и объектовую документацию (журнал учета идентификаторов, инструкции пользователям и др.).

10. Разрабатывать и утверждать в установленном порядке систему мер и действий на случай непредвиденных обстоятельств (заражение объекта ВТ новым типом вируса, фактов НСД к информации, нарушения правил функционирования системы защиты и т.д.).

11. В период профилактических работ на СВТ снимать, при необходимости, комплекс с эксплуатации, о чем делать отметку в формуляре.

12. Принимать меры при попытках НСД к защищаемой информации и нарушении правил функционирования системы защиты. Обязанности администратора БИ должны быть отражены в «Инструкции администратора безопасности информации», утвержденной соответствующим должностным лицом.

Приложение 2.

Принятые термины и сокращения

Администратор БИ	- администратор службы безопасности информации
Имя_пользователя	- имя, под которым пользователь зарегистрирован в системе
Использовать ТМ-идентификатор	- приложить ТМ-идентификатор к контактному устройству съемника информации
Объект доступа	- под объектом доступа понимается один из перечисленных ресурсов СВТ: диск, каталог, файл, процесс (задача), драйвер устройства.
Параметры пользователя	- идентифицирующие признаки пользователя (имя, № ТМ, пароль) и его права по доступу к ресурсам СВТ в соответствии с его полномочиями
Пользователь	- субъект доступа к объектам (ресурсам) СВТ
ПРД	- правила разграничения доступа
Удаление пользователя	- удаление имени, под которым пользователь зарегистрирован в системе, из списка зарегистрированных пользователей в ЭНП контроллера «Аккорд»
Синхронизация параметров пользователя	- сопоставление БД пользователей в ЭНП контроллера «Аккорд» с параметрами БД пользователей подсистемы разграничения доступа и учетными записями пользователей Linux
Создать пользователя	- зарегистрировать пользователя в подсистеме разграничения доступом
Сообщения	- информация, выводимая на дисплей, которая сообщает о действиях пользователя, о состоянии программы и нормально завершенных действиях, сбоях в системе и др.
ТМ-идентификатор (или ТМ)	- персональный идентификатор DS-199x («Touch-memory» – «Память касания») пользователя
Число проходов при удалении	- количество проходов случайной последовательности по содержимому файла при его удалении
ЭНП	- энергонезависимая память контроллера «Аккорд»™