ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО

систем автоматизированного проектирования

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН
11443195.5014-011 99 01-ЛУ

Программно-аппаратные комплексы средств защиты информации от несанкционированного доступа **"АККОРД "**

Подсистема распределенного аудита и управления «Аккорд-РАУ»

Описание применения

11443195.5014-011 99 01

Литера 0_1

АННОТАЦИЯ

Настоящий документ является описанием применения подсистемы распределенного аудита и управления СЗИ «Аккорд» и предназначен для описания механизмов работы ПРАУ.

Распределенный аудит и управление осуществляется на базе программно-аппаратных комплексов средств защиты информации от НСД семейства "Аккорд - АМДЗ" на базе контроллеров "Аккорд-5", "Аккорд-5mx", "Аккорд-5.5", "Аккорд-5.5 Express" и версий специального ПО разграничения доступа "Аккорд-NT/2000", "Аккорд-Win32", или "Аккорд-Win64".

Содержание

Введение

Целями защиты информации являются: предотвращение ущерба, возникновение которого возможно в результате утери (хищения, утраты, искажения, подделки) информации в любом ее проявлении; реализация адекватных угрозам безопасности информации мер защиты в соответствии с действующими Законами и нормативными документами по безопасности информации (НД БИ), потребностями владельцев (пользователей) информации. "Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу".

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

1. ОСНОВНЫЕ ПРИНЦИПЫ ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД

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. 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 ее 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 должностным предназначением;

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

7. Обеспечение физической охраны объекта, 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, администратор АС), 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.

2. ОБЩИЕ СВЕДЕНИЯ

Подсистемы распределенного аудита и управления (далее Аккорд-РАУ) состоит их двух частей. Основная часть - автоматизированное рабочее место администратора безопасности информации (АРМ АБИ) на базе комплекса "Аккорд-АМДЗ" устанавливается на отдельном компьютере, а на рабочих станциях дополнительно к СПО «Аккорд» устанавливается клиент РАУ. АРМ АБИ предназначено для оперативного наблюдения за работой пользователей, оперативного управления рабочими станциями и составом пользователей СЗИ, централизованного сбора журналов регистрации работы комплексов "Аккорд-NT/2000", "Аккорд-Win32", или "Аккорд-Win64" (далее комплекс, или ПАК СЗИ "Аккорд") .

СЗИ "Аккорд" обеспечивает для пользователя "прозрачный" режим работы, при котором пользователь, как правило, не замечает внедренной системы защиты. При этом, дополнительная нагрузка, связанная с эксплуатацией СЗИ, не ложится на пользователя, а замыкается на администраторе безопасности информации (БИ). В этой связи для обеспечения эффективности работы АС администратор БИ обязан досконально изучить и правильно применять возможности системы защиты информации на базе СЗИ "Аккорд".

Использование ПЭВМ с внедренными средствами защиты комплекса не требует изменения существующего программного обеспечения, необходимы лишь квалифицированное применение комплекса (правильная установка, настройка и эксплуатация в соответствии с принятыми на предприятии ПРД) и обеспечение некоторой организационной поддержки.

Как показывает практика довольно длительного применения комплекса, 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 ПЭВМ (АС) 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 технических средств защиты информации, в том числе и комплекса "Аккорд", необходима специальная служба (администрация) безопасности информации (СБИ), в небольших организациях и подразделениях - администратор безопасности информации (АБИ). На СБИ (администратора БИ) возлагаются задачи по

осуществлению единого руководства, организации применения средств защиты и управления ими, а также контроль за соблюдением всеми категориями пользователей требований по обеспечению безопасности программно-информационных ресурсов автоматизированных систем.

АРМ АБИ предназначен для оперативного наблюдения и управления за работой пользователей ПАК СЗИ семейства Аккорд, работающих в составе ЛВС.

АБИ имеет возможность наблюдать за пользователями, работающими под контролем ПАК СЗИ "Аккорд" в составе ЛВС. В любой момент времени АБИ может получить информацию о том, кто работает на данной станции, версию операционной системы, под управлением которой идет работа, список задач, которые выполняются на этой станции в текущий момент времени.

Кроме того, на АРМ АБИ происходит получение журналов регистрации работ ПАК СЗИ "Аккорд" в режиме реального времени, то есть все попытки НСД тут же отображаются на экране АРМ АБИ.

АБИ может просматривать все события со всех станций в одном окне. Но если возникает необходимость детального анализа работы одной станции, то можно все поступающие события выводить в отдельное окно.

Для улучшения восприятия информации, АБИ может воспользоваться системой фильтров, которые позволят выбрать только те рабочие станции или только те события, которые вызывают в данный момент времени особенных интерес.

Для лучшего понимания того, что происходит на какой-либо станции, АБИ может оперативно изменить уровень детальности журнала. Или, в случае необходимости, просмотреть экран выбранной рабочей станции.

Администратор безопасности может выбрать в настройках программы режим отправки сообщений о несанкционированном доступе на определенный адрес электронной почты.

С помощью АРМ администратор безопасности информации может выполнять следующие функции:

- оперативное наблюдение за работой пользователей,
- оперативное управление работой пользователей,
- централизованный сбор журналов регистрации СЗИ НСД Аккорд,
- изменение списка зарегистрированных рабочих станций и серверов.

3. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

	Контроллер	версия ПО	версия BIOS контроллера
АРМ администратора	Аккорд – АМДЗ (на базе контроллеров 5, 5mx, 5.5)	Драйвер контроллера, ПО АРМ АБИ	v.1.40, 1.41, 2.20
Рабочая станция	Аккорд – АМДЗ (на базе контроллеров 5, 5mx, 5.5)	"Аккорд-NT/2000", "Аккорд-Win32", "Аккорд-Win64"	v.1.40, 1.41, 2.20
Сервер	Аккорд – АМДЗ (на базе контроллеров 5, 5mx, 5.5)	"Аккорд-NT/2000", "Аккорд-Win32", "Аккорд-Win64"	v.1.40, 1.41, 2.20

Система функционирует в локальных, или распределенных сетях с использованием протоколов TCP/IP, или IPX.

4. Функциональные обязанности администратора безопасности.

4.1 Оперативное управление

В случае обнаружения попытки НСД АБИ имеет возможность:

- послать сообщение пользователю;
- включить ему хранитель экрана, который может быть разблокирован только ТМ-идентификатором АБИ;
- перегрузить рабочую станцию.

4.2 Централизованный сбор журналов регистрации событий комплекса «Аккорд»:

АБИ может со своего рабочего места получать журналы регистрации событий комплекса "Аккорд. Для этого ему достаточно выбрать соответствующий пункт меню АРМ АБИ и выбрать станции, с которых необходимо получить журналы. Все полученные журналы будут перемещены в подкаталог, соответствующий имени станции и дате выполнения операции. После этого журналы становятся доступными для просмотра и архивирования.

4.3 Управление составом пользователей и набором их ПРД на рабочих станциях

Администратор может редактировать базы пользователей на рабочих станциях. База данных копируется на АРМ АБИ, и открывается программа - редактор ПРД. Измененные базы рассылаются на отмеченные администратором рабочие станции после завершения работы программы – редактора. При установке соответствующих параметров настройки комплекса на рабочей станции после получения базы пользователей может выполняться синхронизация с контроллером АМДЗ и составом пользователей в ОС.

Внимание !
Доступ к журналам и списку пользователей в контроллере АМДЗ имеет только администратор. Для выполнения операций получения журналов и редактирования пользователей идентификатор администратора, который предъявляется при запуске АРМ АБИ, должен быть зарегистрирован в контроллерах «Аккорд-АМДЗ» в группе «Администраторы» на всех рабочих станциях.

4.4 Управление списком рабочих станций и серверов.

Все рабочие станции и сервера, управляемые с АРМ АБИ, согласно технологии усиленной аутентификации должны содержать файл acnode.lst. Синхронизация содержимого этого файла выполняется соответствующей командой на АРМ АБИ. Удаление рабочей станции из списка делает невозможным обмен информацией между защищенным компьютером и АРМ АБИ.