ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО

систем автоматизированного проектирования

УТВЕРЖДЕН

11443195.509000.047 31-ЛУ

СПЕЦИАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА «АККОРД-Х К»

ОПИСАНИЕ ПРИМЕНЕНИЯ 11443195.509000.047 31

Подпись и дата	
Инв. № дубл.	
Взам. инв. №	
Подпись и дата	
Инв. № подл.	

Изм	Лист	№ документа	Подпись	Дата	11443195.509000.047 31			
Разработ.					СПЕЦИАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА «АККОРД-Х К». ОПИСАНИЕ ПРИМЕНЕНИЯ	Лит.	Лист	Листов
Проверил						$О_1$	1	1
Т.контр.						ОКБ САПР		
Н.контр.								
Утвердил								

АННОТАЦИЯ

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

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

Перед установкой и эксплуатацией СПО «Аккорд-X K» необходимо внимательно ознакомиться с комплектом эксплуатационной документации, а также принять необходимые организационные меры защиты, указанные в документации.

Применение защитных механизмов СПО «Аккорд-X K» должно дополняться общими мерами предосторожности и физической безопасности СВТ.

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ

Специальное программное обеспечение «Аккорд-X K» (далее по тексту – СПО «Аккорд-X K», «Аккорд-X K») предназначено для применения в СВТ типа IBM PC (автономных ПК, рабочих станциях ЛВС, терминальных серверах), функционирующих под управлением ОС семейства Linux, с целью обеспечения защиты от несанкционированного доступа к информации при многопользовательском режиме эксплуатации.

СПО «Аккорд-X K» предназначено для выполнения основных функций защиты от НСД на основе:

- применения парольного механизма;
- реализации механизмов разграничения доступа;
- контроля целостности критичных с точки зрения информационной безопасности программ и данных. В программной части СЗИ НСД возможна проверка целостности программ и данных по индивидуальному списку для отдельного пользователя, или группы пользователей. Подсистема контроля целостности предусматривает как статический список (проверка выполняется однократно в начале сеанса), так и динамический список, проверка по которому выполняется перед каждой загрузкой контролируемого файла в оперативную память;
- очистки внешней памяти;
- механизма регистрации действий пользователей в системном журнале, доступ к которому предоставляется только Администратору БИ.

2 ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ И ОРГАНИЗАЦИОННЫЕ МЕРЫ, НЕОБХОДИМЫЕ ДЛЯ ПРИМЕНЕНИЯ СПО «АККОРД-X K»

2.1 Технические требования

Для установки СПО «Аккорд-X K» требуется следующий минимальный состав технических и программных средств:

- IBM PC AT, совместимая с процессором и объемом RAM, обеспечивающим применение операционных систем Linux;
- объем дискового пространства для установки СПО – не менее 128 Мб.

2.2 Организационные меры

Для эффективного применения СПО «Аккорд-X K» и поддержания необходимого уровня защищенности СВТ (РС) и информационных ресурсов АС **необходимо**[1]**:**

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

[1] Более подробно приведены в документах «Руководство администратора» (11443195.509000.047 90) и «Руководство оператора (пользователя)» (11443195.509000.047 34)

3 ОСОБЕННОСТИ ЗАЩИТНЫХ ФУНКЦИЙ СПО «АККОРД-X K»

Защитные функции СПО «Аккорд-X K» реализуются применением:

1) Дисциплины защиты от НСД СВТ (РС), включая:

- идентификацию пользователя по уникальным данным для идентификации;
- аутентификацию с учетом необходимой длины пароля;
- ограничение времени доступа субъекта к СВТ (АС) в соответствии с установленным режимом работы пользователей.

2) Дисциплины разграничения доступа к ресурсам СВТ (АС) в соответствии с установленными ПРД и определяемыми атрибутами доступа, которые устанавливаются администратором безопасности информации (Администратором БИ) соответственно каждой паре «субъект доступа - объект доступа» при регистрации пользователей. СПО «Аккорд-X K» позволяет Администратору БИ использовать как дискреционный метод разграничения, так и контроль доступа на основе иерархических меток;

3) Контроля целостности критичных с точки зрения информационной безопасности программ и данных (дисциплины защиты от несанкционированных модификаций). В программной части СЗИ НСД возможна проверка целостности программ и данных по индивидуальному списку для отдельного пользователя, или группы пользователей. Подсистема контроля целостности предусматривает как статический список (проверка выполняется однократно в начале сеанса), так и динамический список, проверка по которому выполняется перед каждой загрузкой контролируемого файла в оперативную память;

4) Механизма очистки внешней памяти.

5) Регистрации действий пользователей в системном журнале, доступ к которому предоставляется только Администратору БИ.

4 ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ СПО «АККОРД-Х К»

Схема построения системы защиты информации с использованием СПО «Аккорд-Х К» и ее взаимодействие с программно-аппаратным обеспечением СВТ показаны на рисунке 1.

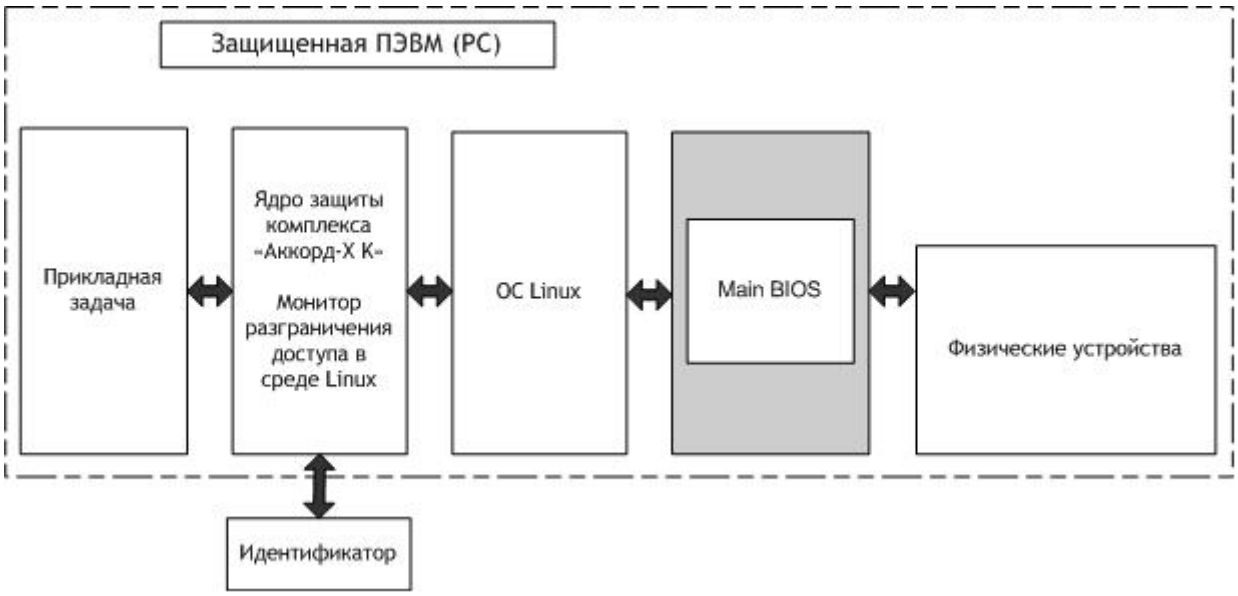

Рисунок 1 - Схема построения системы защиты информации

Защита информации с использованием средств «Аккорд-Х К» основана на обработке событий, возникающих при обращении прикладных программ или системного ПО к ресурсам СВТ. Средства СПО «Аккорд-Х К» перехватывают соответствующие программные 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).

СПО «Аккорд-Х К» 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).

Рисунок 2 - Состав СПО «Аккорд-X K»

4.1 Подсистема управления доступом

Подсистема управления доступом предназначена для защиты СВТ от посторонних[1] 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 предъявленных данных для идентификации с перечнем зарегистрированных на СВТ) и аутентификации (подтверждение подлинности) с защитой от раскрытия пароля.

В СПО «Аккорд-X K» реализованы принципы дискреционного контроля доступа и контроля доступа на основе иерархических меток.

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

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

Возможно использование одновременно двух механизмов доступа.

[1] Под посторонними пользователями понимаются все лица, не зарегистрированные в системе.

Настройка подсистемы разграничения доступом СПО «Аккорд-X K» осуществляется Администратором БИ с использованием утилиты acx-admin (см. документ «Руководство администратора» (11443195.509000.047 90), входящий в состав эксплуатационной документации на СПО «Аккорд-X K»).

4.2 Подсистема регистрации и учета

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

При регистрации событий в системном журнале указываются:

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

Перечень регистрируемых событий, их описание приводится в документе «Руководство администратора» (11443195.509000.047 90).

Работа с системными журналами осуществляется с использованием утилиты acx-admin log (см. документ «Руководство администратора» (11443195.509000.047 90), входящий в состав эксплуатационной документации на СПО «Аккорд-X K»).

В Н И М А Н И Е !

Доступ к системному журналу возможен только Администратору БИ

4.3 Подсистема обеспечения целостности

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

Контроль целостности в СПО «Аккорд-X K» реализуется путем:

- проверки целостности назначенных для контроля системных файлов, пользовательских программ и данных;
- создания замкнутой программной среды, запрещающей запуск измененных программ.

Функционирование подсистемы обеспечения целостности в «Аккорд-X K» 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 могут изменяться в процессе эксплуатации СВТ;
- для исключения фактов не обнаружения модификации файла используется алгоритм расчета контрольных сумм.

5 СОСТАВ СПО «АККОРД-Х К»

Состав специального программного обеспечения «Аккорд-Х К» приведен в документе «Описание программы» (11443195.501410.047 13).

6 ПРИНЦИП РАБОТЫ СПО «АККОРД-Х К»

Активизация монитора разграничения доступа, регистрация пользователей и установка правил разграничения доступа выполняются только Администратором БИ.

При регистрации пользователей Администратором БИ определяются их права доступа: список исполняемых программ и модулей, разрешенных к запуску данным пользователем, и список прав доступа к объектам (ресурсам) с использованием дискреционного механизма разграничения и/или контроля доступа на основе иерархических меток (см. документ «Руководство администратора» (11443195.509000.047 90)).

С помощью утилиты acx-admin в специальный файл данных вносятся списки файлов, целостность которых будет проверяться при запуске СВТ (РС) данным пользователем.

Особенностью и, несомненно, преимуществом СПО «Аккорд-Х К» является проведение процедур идентификации, аутентификации и контроля целостности (программных компонентов, файлов).

После предъявления данных для идентификации выполняется процедура аутентификации (ввод пароля) пользователя. Для проведения процедуры аутентификации пароль вводится в виде символов <*>.

С данными, полученными в результате идентификации/аутентификации пользователей, выполняется процедура хеширования.

Далее выполняется поиск свертки идентификационных параметров пользователя в базе данных СПО «Аккорд-Х К». Если предъявлены зарегистрированные данные для идентификации и пароль введен правильно, то выполняется контроль целостности защищаемых объектов.

При положительном результате контрольных процедур пользователю становится доступной процедура входа в ОС. Если предъявленные пользователем данные для идентификации не зарегистрированы в списке (сообщения «Недопустимый идентификатор», «Ошибка чтения идентификатора») или нарушена целостность защищаемых объектов (сообщение «Нарушение целостности»), пользователь не сможет выполнить вход в ОС. Для продолжения работы потребуется вмешательство Администратора БИ.

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

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

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

Важной составляющей безопасности при работе операционной системы является динамический контроль целостности процессов (задач) в оперативной памяти СВТ (РС). Администратор БИ может задать список процессов для динамического контроля, и в процессе функционирования СПО «Аккорд-Х К» резидентная часть монитора разграничения доступа проверяет загружаемый процесс и обеспечивает оперативный контроль целостности исполняемых файлов

перед передачей им управления. Тем самым обеспечивается защита от программных вирусов и закладок. В случае положительного исхода проверки управление передается операционной системе и процесс запускается на исполнение. При отрицательном исходе проверки загрузка и запуск задачи не происходит.

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

7 ПОСТАВКА СПО «АККОРД-Х К»

Комплект поставки СПО «Аккорд-Х К» приведен в формуляре (11443195.509000.047 ФО).

8 УСТАНОВКА И НАСТРОЙКА СПО «АККОРД-Х К»

Установка СПО «Аккорд-Х К» и его настройка с учетом особенностей политики информационной безопасности, принятой на объекте Заказчика, осуществляется, как правило, специалистами по защите информации организации (предприятия, фирмы и т.д.) в соответствии с требованиями эксплуатационной документации на СПО «Аккорд-Х К».

Установка и настройка СПО «Аккорд-Х К» осуществляется Администратором БИ в соответствии с документом «Руководство администратора» (11443195.509000.047 90).

9 УПРАВЛЕНИЕ ЗАЩИТОЙ ИНФОРМАЦИИ

Созданная структура защиты информации при применении СПО «Аккорд-Х К» должна поддерживаться механизмом установления полномочий пользователей СВТ (АС) и управлением их доступом к информационным ресурсам защищаемой АС.

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

Перечень организационных мер, необходимых для обеспечения СПО «Аккорд-Х К» требуемого уровня защиты информации, а также функции и обязанности Администратора БИ и пользователей приведены в документах «Руководство администратора» (11443195.509000.047 90) и «Руководство оператора (пользователя)» (11443195.509000.047 34).