ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
ОКБ АПР систем автоматизированного проектирования

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

Специальное программное обеспечение средств защиты информации от несанкционированного доступа «Аккорд-X K»

РУКОВОДСТВО ОПЕРАТОРА (ПОЛЬЗОВАТЕЛЯ)

37222406.26.20.40.140.085 34

Москва
2023

АННОТАЦИЯ

Руководство предназначено для конкретизации действий операторов (пользователей) при эксплуатации специального программного обеспечения средств защиты информации от несанкционированного доступа (СПО СЗИ НСД) «Аккорд-X K» (ТУ 509000-047-11443195-2011) (далее по тексту – СПО СЗИ НСД «Аккорд-X K», СПО «Аккорд-X K», «Аккорд-X K») и содержит описание способов использования средств защиты СПО «Аккорд-X K», его интерфейса с пользователем в процессе обработки информации.

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

Применение защитных механизмов СПО «Аккорд-X K» должно дополняться общими мерами технической безопасности, а также физической охраной СВТ и его ресурсов.

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ О СПО «АККОРД-X K»

1.1 Состав СПО «Аккорд-X K»

Специальное программное обеспечение «Аккорд-X K» (далее по тексту СПО «Аккорд-X K», «Аккорд-X K») представляет собой программное средство, предназначенное 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.

1.2 Назначение СПО «Аккорд-X K»

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

- применения парольного механизма;
- реализации механизмов разграничения доступа и обеспечения управления потоками информации, исключая возможность её несанкционированного переноса из объектов с меньшим уровнем конфиденциальности в объекты с большим уровнем;
- 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.

1.3 Технические условия применения СПО «Аккорд-X K»

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

1) IBM PC AT, совместимая с процессором и объемом RAM, обеспечивающим применение операционных систем Linux;

2) объем дискового пространства для установки СПО – не менее 128 Мб.

2 ПОРЯДОК РАБОТЫ НА ЗАЩИЩЕННОМ СВТ

Процесс работы пользователя на СВТ, защищенном СПО «Аккорд-X K», можно разделить на следующие этапы:

1) выполнение контрольных процедур;

2) работа пользователя в соответствии с функциональными обязанностями и правами доступа;

3) завершение работы и выход из системы.

ВНИМАНИЕ!

Работа в ОС Linux с установленным СПО «Аккорд-X K» отличается (от работы в ОС без СПО «Аккорд-X K») только необходимостью ввода специальных данных для идентификации и аутентификации и возможными запретами на получение доступа к какому-либо объекту или файлу.

2.1 Выполнение контрольных процедур

Контрольные процедуры делятся на обязательные, выполняемые при каждом запуске СВТ и необязательные, выполняемые при выполнении заданных условий.

К обязательным процедурам относятся

- процедура идентификации;
- процедура аутентификации;
- проверка целостности системных файлов, программ и данных.

2.1.1 Процедура идентификации

В момент запуска подсистемы разграничения доступа может выполняться контроль целостности файлов, по индивидуальному списку каждого пользователя. В случае если контрольные процедуры завершились успешно, то происходит загрузка СПО «Аккорд-X K», и на экран выводится соответствующая информация (рисунок 1) (в случае какой-либо ошибки возникает паника ядра с указанием причины – превышен таймер ожидания БД, неправильная лицензия и т.п. – и дальнейшая загрузка ОС не осуществляется). После этого активируются и вступают в действие механизмы защиты, которые включены в данных о конфигурации МРД (их может изменить Администратор БИ в ходе работы ОС с использованием утилиты acx-admin). Необходимо отметить, что для пользователя все указанные действия могут быть невидимы - защитные механизмы не оказывают воздействия на быстродействие ОС, а экран с информацией о ходе начальной загрузки (рисунок 1) в зависимости от быстродействия СВТ может сменяться достаточно быстро.

Процесс входа в ОС: загрузка модуля разграничения доступа, выполнение процедур идентификации и аутентификации.

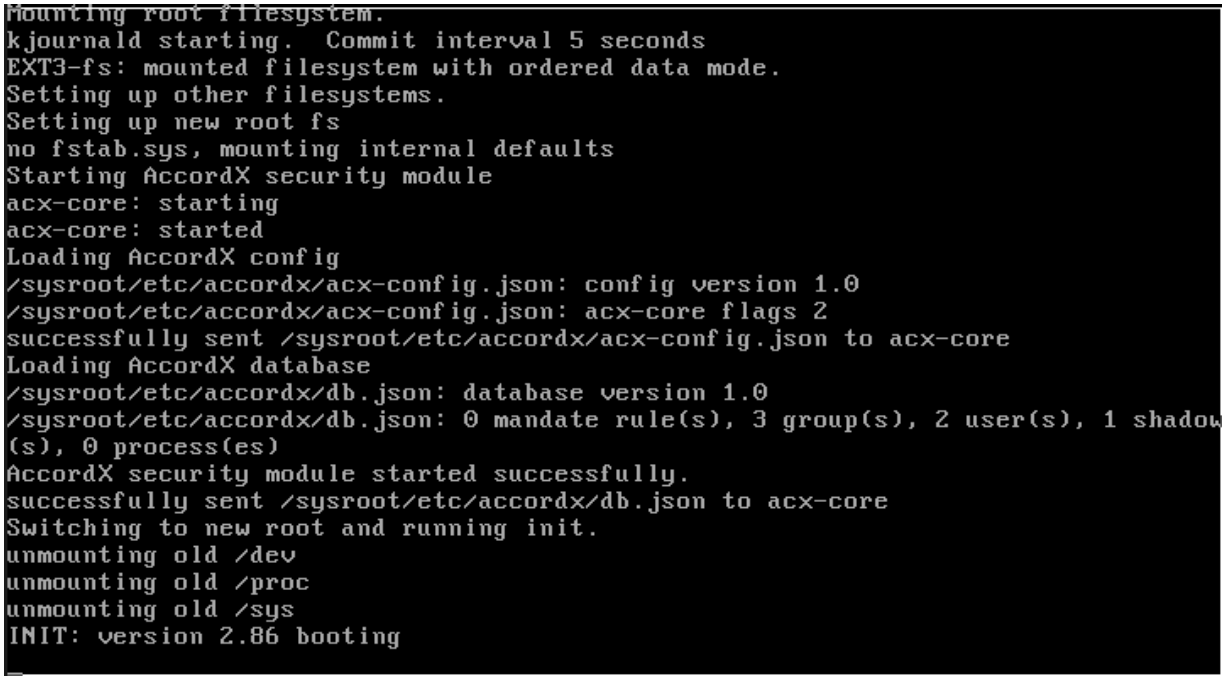

Рисунок 1 - Загрузка модуля разграничения доступа «Аккорд-X K»

На заключительном этапе загрузки ОС выводится окно приветствия (стандартное окно входа в ОС, внешний вид отличается в различных дистрибутивах) (рисунок 2). Необходимо ввести данные для идентификации или предъявить соответствующий идентификатор пользователя.

В Н И М А Н И Е !

Выполнять подключение к ОС zLinux можно по протоколу ssh с помощью одноименной утилиты из пакета acx-remote (предварительно подтвердив ключ zLinux с помощью стандартного ssh-клиента), дополнительно предъявляя аппаратные идентификаторы, поддерживаемые соответствующим пакетом acx-tmid-*.

Рисунок 2 - Запрос данных для идентификации

2.1.2 Процедура аутентификации

После предъявления данных для идентификации (в случае если не произошло ошибки считывания) в появившемся поле «Введите пароль» следует ввести соответствующий пароль пользователя, установленный для него в «Аккорд-X K» (рисунок 3).

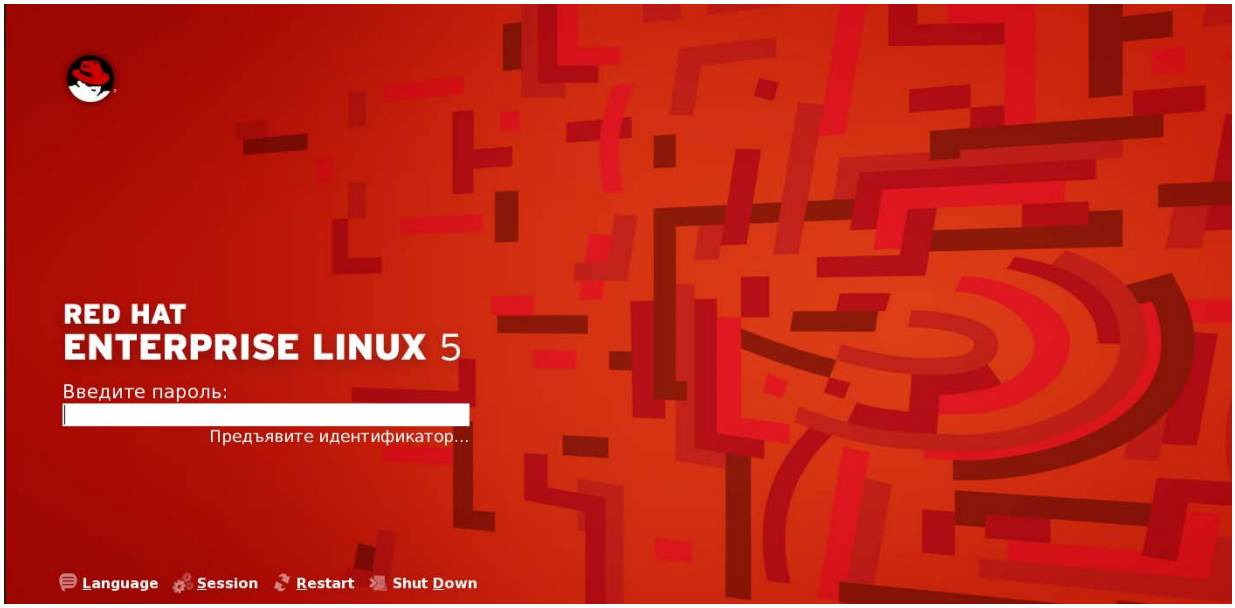

Рисунок 3 - Запрос пароля

В случае наличия пары «данные для идентификации/данные для аутентификации» для пользователя в СПО «Аккорд-X K» процесс идентификации и аутентификации завершается успешно, при этом осуществляется стандартный вход в ОС.

Сразу после выполнения процедуры идентификации/аутентификации пользователя начинают работать соответствующие правила разграничения доступа, которые ранее были заданы Администратором БИ конкретно для данного пользователя.

2.1.3 Проверка целостности системных файлов, программ и данных

Данная процедура предназначена для исключения несанкционированных модификаций (случайных или злоумышленных) программной среды СВТ, системных файлов ОС, обрабатываемых пользователем данных, если они поставлены на контроль целостности.

При проверке на целостность вычисляется контрольная сумма файлов и сравнивается с эталонным значением. Эти данные заносятся при регистрации пользователя и могут меняться в процессе эксплуатации СВТ.

В случае если нарушена целостность защищаемых файлов, на экран выводится соответствующее сообщение, и дальнейшая загрузка ОС не производится. Загрузка будет возможна только для администратора.

В ходе загрузки ОС дополнительно может проводиться статический контроль целостности данных, поставленных на контроль Администратором БИ в СПО «Аккорд-X K». Также во время обычной работы пользователя может выполняться динамический контроль целостности открываемых на выполнение файловых объектов. Все эти операции могут быть незаметными для пользователя (заметить их можно только по вторичным признакам - ошибка при входе в ОС, невозможность запуска приложения и т.д.). В случае возникновения каких-либо проблем необходимо обратиться к Администратору БИ (или см. «Руководство администратора» на СПО «Аккорд-X K»).

2.2 Работа пользователя в соответствии с функциональными обязанностями

После выполнения контрольных процедур выполняется загрузка операционной системы, и пользователь может приступить к работе, определяемой его функциональными обязанностями и правами доступа к ресурсам СВТ.

При регистрации пользователя для него создается функционально замкнутая программная среда, которая позволяет контролировать права доступа пользователя к объектам доступа.

2.2.1 Проверка полномочий по доступу

Выполняется при запуске пользователем какой-либо программы или при попытке получить доступ к какому-либо ресурсу. Средствами СПО «Аккорд-X K» выполняется проверка полномочий пользователя, которая заключается в том, что в списке прав доступа пользователя осуществляется поиск описания данного ресурса.

Если в списке прав доступа пользователя разрешена работа с данной программой или файлом, то пользователь может легально работать в соответствии со своими функциональными обязанностями.

Если в списке прав доступа пользователя не разрешена работа с данной программой или файлом (или ограничен набор функций, которые может выполнить пользователь с данным ресурсом), то выводится стандартное сообщение операционной системы, например, «Файл не найден», «Невозможно удалить файл» и т. д.

2.3 Завершение работы и выход из системы

Завершение работы прикладных программ происходит в порядке, установленном для конкретного прикладного программного обеспечения, описанном в соответствующих руководствах. Никаких специфических окон или сообщений «Аккорд-X K» при этом не выводит.

3 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

В случае необходимости консультации АО «ОКБ САПР» предлагает без дополнительной оплаты с понедельника по пятницу с 10-00 до 18-00 (по московскому времени) обращаться по телефонам:

+7 (495) 994-49-96

+7 (495) 994-49-97

+7 (926) 762-17-72

или по адресам электронной почты: support@okbsapr.ru, help@okbsapr.ru.

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

Приложение 1. ОБЯЗАННОСТИ ДОЛЖНОСТНЫХ ЛИЦ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ВЫПОЛНЕНИИ РАБОТ НА СВТ

ОБЩИЕ ТРЕБОВАНИЯ

Все должностные лица (сотрудники) организации должны быть ознакомлены с этой инструкцией и своими обязанностями по обеспечению безопасности информации при выполнении ими работ на СВТ.

Персонал, допущенный к автоматизированной обработке конфиденциальной информации, обязан строго соблюдать установленные правила работы на автоматизированных рабочих местах и несет персональную ответственность за обеспечение безопасности информации при работе на технических средствах автоматизированной системы.

Установление личной ответственности сотрудников за поддержание уровня защищенности СВТ при обработке сведений, подлежащих защите по действующему законодательству, происходит путем:

- ознакомления с перечнем защищаемых сведений, организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации;

- определения уровня полномочий в соответствии с его должностными обязанностями;

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

Мера ответственности персонала за выполнение действий, нарушающих политику безопасности, определяется нанесенным ущербом, наличием злого умысла и некоторыми субъективными факторами по усмотрению руководства учреждения (дисциплинарная, административная или уголовная).

Любое нарушение порядка и правил работы персоналом АС должно тщательно расследоваться, а к виновным должны применяться необходимые меры воздействия.

Все компоненты программного и аппаратного обеспечения системы должны использоваться персоналом ТОЛЬКО в служебных целях. Использование их в других целях ЗАПРЕЩАЕТСЯ.

Запрещается прием посетителей в помещениях, когда в них осуществляется обработка конфиденциальной информации на СВТ.

Пользователям ЗАПРЕЩАЕТСЯ самовольно изменять конфигурацию аппаратно-программных средств или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формулярами рабочих мест и планом защиты. Исключением являются только те случаи, когда пользователь имеет права администратора (супервизора).

Все изменения конфигурации технических и программных средств осуществляются только на основании решения руководства организации

персоналом из числа инженеров, системных и прикладных программистов с участием администратора безопасности АС.

О случаях обнаружения непредусмотренных отводов кабелей и проводов, изменений алгоритмов функционирования технических и программных средств СВТ, нарушениях нормальной работы средств защиты, которые свидетельствуют о возможных попытках или фактах НСД к информации, необходимо немедленно ставить в известность администратора безопасности.

Любые изменения состава и конфигурации технических средств и программного обеспечения должны быть предварительно проанализированы на предмет их соответствия политике безопасности. Все добавляемые компоненты должны быть проверены на работоспособность, отсутствие вирусов и специальных вложений, а также отсутствие реализации опасных функций.

После изменения конфигурации СВТ в обязательном порядке должен производиться пересмотр существующих инструкций пользователей по обеспечению безопасности.

Категорически запрещается записывать и хранить конфиденциальную информацию на неучтенных гибких магнитных дисках, а также использовать гибкие магнитные диски с выявленными неисправностями.

ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

В обязанности пользователей входит своевременный и точный ввод данных в систему и активизация процесса их обработки. Пользователи обладают правами доступа к системе и имеют возможность вводить и корректировать необходимую информацию. Они несут ответственность за содержание вводимой ими информации.

Пользователь (ответственный исполнитель работ) несет ответственность за сохранность и правильное использование получаемых в ходе выполнения работ машинных носителей и машинных документов с конфиденциальной информацией.

Степень конфиденциальности гибких магнитных дисков и машинных документов, получаемых в ходе автоматизированной обработки информации с помощью СВТ, определяется должностным лицом, выдавшим задание на автоматизированную обработку информации.

По окончании рабочего дня полученные во временное пользование гибкие магнитные диски (при необходимости и идентификаторы) должны быть возвращены в_____
(название подразделения, ответственного за хранение ГМД и идентификаторов).

Необходимо производить стирание с магнитных носителей конфиденциальной информации, не предназначенной для дальнейшего использования. Стирание информации производится допущенным к ее автоматизированной обработке должностным лицом под контролем администратора безопасности с отметкой в журнале учета стирания информации с магнитных машинных носителей.

После окончания обработки конфиденциальной информации и изъятия гибкого магнитного диска из дисковода необходимо выключить электропитание СВТ.

Ответственный за СВТ (АРМ) обязан проверять целостность и соответствие печатей в начале и по окончании рабочего дня.

Пользователям ЗАПРЕЩАЕТСЯ самовольно изменять конфигурацию аппаратно-программных средств или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формулярами рабочих мест и планом защиты.

В случае выявления сбоев и ошибок в процессе эксплуатации изделия пользователь должен незамедлительно прекратить его использование и сообщить об этом ответственному лицу - администратору служба безопасности информации (СБИ) или администратор безопасности информации (АБИ).