

ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО



систем автоматизированного
проектирования

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН
11443195.509000.047 34 -ЛУ

Специальное программное обеспечение
средств защиты информации от
несанкционированного доступа
«**АККОРД-Х К**» (версия 1.0)

**РУКОВОДСТВО ОПЕРАТОРА
(ПОЛЬЗОВАТЕЛЯ)**

11443195.509000.047 34

Москва
2016

АННОТАЦИЯ

Руководство предназначено для конкретизации действий операторов (пользователей) при эксплуатации специального программного обеспечения средств защиты информации от несанкционированного доступа (СПО СЗИ НСД) «Аккорд-Х К» v.1.0 (ТУ 509000-047-11443195-2008) (далее по тексту – СПО СЗИ НСД «Аккорд-Х К», СПО «Аккорд-Х К», «Аккорд-Х К») и содержит описание способов использования средств защиты СПО «Аккорд-Х К», его интерфейса с пользователем в процессе обработки информации.

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

Применение защитных механизмов СПО «Аккорд-Х К» должно дополняться общими мерами технической безопасности, а также физической охраной СВТ и ее средств.

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ ОБ СПО «АККОРД-Х К».....	4
1.1 Состав СПО «Аккорд-Х К».....	4
1.2 Назначение СПО «Аккорд-Х К».....	4
1.3 Технические условия применения СПО «Аккорд-Х К».....	4
2 ПОРЯДОК РАБОТЫ НА ЗАЩИЩЕННОЙ СВТ	4
2.1 Выполнение контрольных процедур.....	5
2.1.1 Процедура идентификации.....	5
2.1.2 Процедура аутентификации.....	6
2.1.3 Проверка целостности системных файлов, программ и данных	7
2.2 Работа пользователя в соответствии с функциональными обязанностями.....	8
2.2.1 Проверка полномочий по доступу	8
2.3 Завершение работы и выход из системы.....	8

1 ОБЩИЕ СВЕДЕНИЯ ОБ СПО «АККОРД-Х К»

1.1 Состав СПО «Аккорд-Х К»

Специальное программное обеспечение «Аккорд-Х К» (далее по тексту СПО «Аккорд-Х К», «Аккорд-Х К») 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-Х К»

СПО «Аккорд-Х К» 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-Х К»

Для установки СПО «Аккорд-Х К» 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 ЗАЩИЩЕННОЙ СВТ

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

11443195.509000.026 34

- 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-Х К» отличается (от работы в ОС без СПО «Аккорд-Х К») 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-Х К» 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 `asx-admin`). Необходимо отметить, что для пользователя все указанные действия могут быть невидимы - защитные механизмы не оказывают воздействия на быстроедействие ОС, а экран с информацией о ходе начальной загрузки (рисунок 1) в зависимости от быстрогодействия СВТ может сменяться достаточно быстро.

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

```
Mounting root filesystem.
kjournald starting. Commit interval 5 seconds
EXT3-fs: mounted filesystem with ordered data mode.
Setting up other filesystems.
Setting up new root fs
no fstab.sys, mounting internal defaults
Starting AccordX security module
acx-core: starting
acx-core: started
Loading AccordX config
/sysroot/etc/accordx/acx-config.json: config version 1.0
/sysroot/etc/accordx/acx-config.json: acx-core flags 2
successfully sent /sysroot/etc/accordx/acx-config.json to acx-core
Loading AccordX database
/sysroot/etc/accordx/db.json: database version 1.0
/sysroot/etc/accordx/db.json: 0 mandate rule(s), 3 group(s), 2 user(s), 1 shadow
(s), 0 process(es)
AccordX security module started successfully.
successfully sent /sysroot/etc/accordx/db.json to acx-core
Switching to new root and running init.
unmounting old /dev
unmounting old /proc
unmounting old /sys
INIT: version 2.86 booting
```

Рисунок 1 – Загрузка модуля разграничения доступа «Аккорд-Х К»

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.

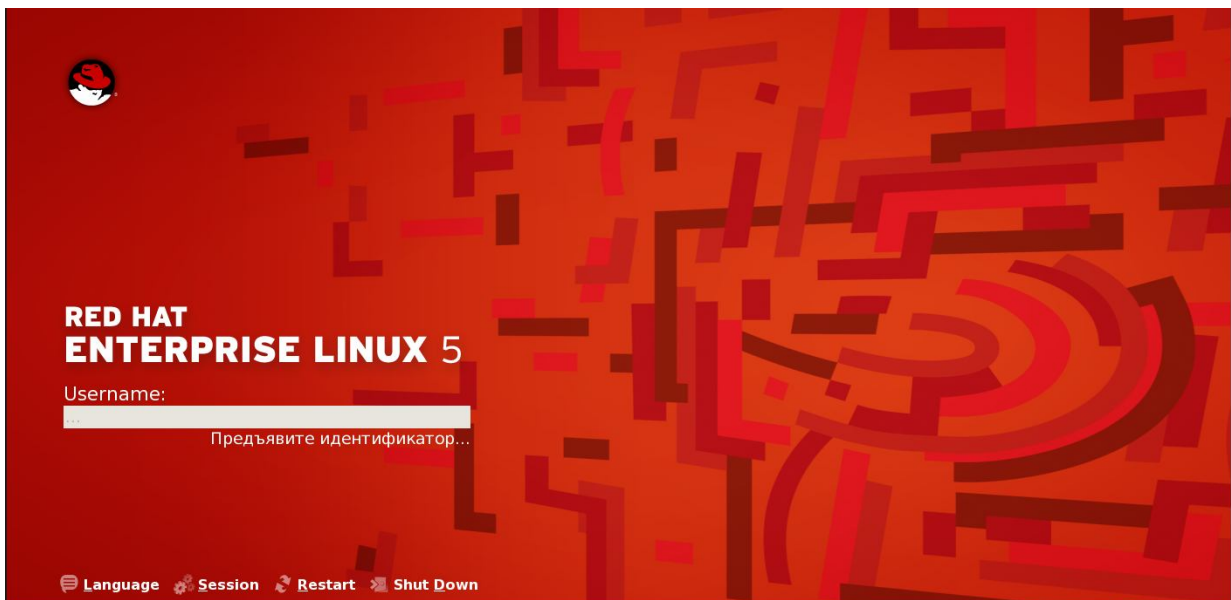


Рисунок 2 – Запрос данных для идентификации

2.1.2 Процедура аутентификации

После предъявления данных для идентификации (в случае если не произошло ошибки считывания) в появившемся поле «Введите пароль» следует ввести

11443195.509000.026 34

соответствующий пароль пользователя, установленный для него в «Аккорд-Х К» (рисунок 3).

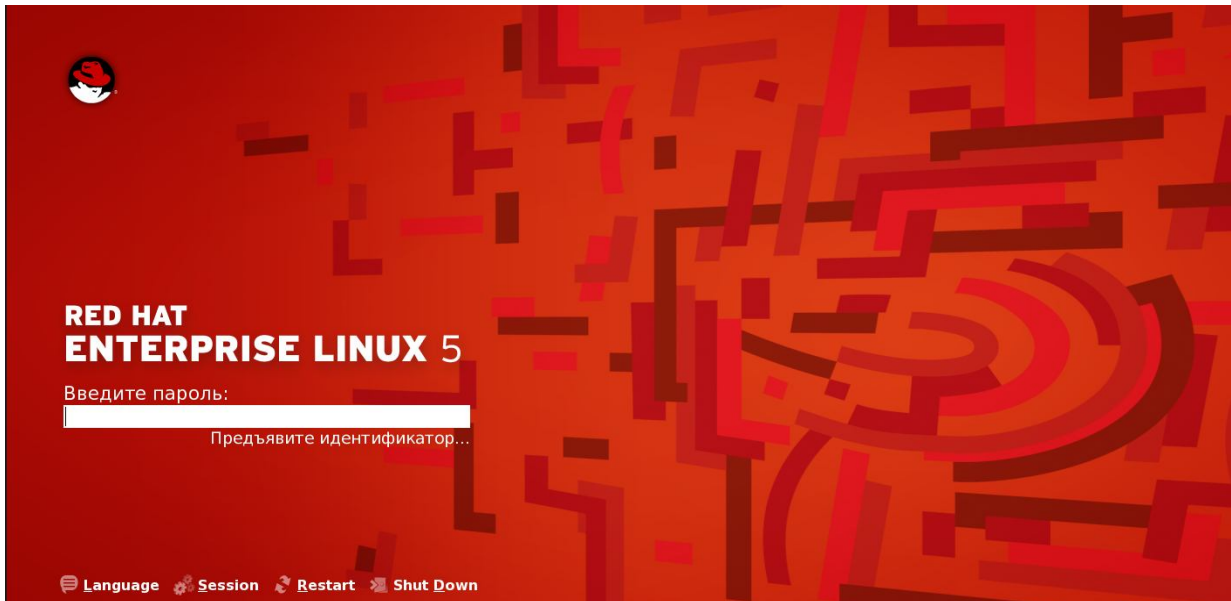


Рисунок 3 – Запрос пароля

В случае наличия пары «данные для идентификации/данные для аутентификации» для пользователя в СПО «Аккорд-Х К», 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-Х К». 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

11443195.509000.026 34

т.д.). В случае возникновения каких-либо проблем необходимо обратиться к Администратору БИ (или см. «Руководство администратора» на СПО «Аккорд-Х К»).

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-Х К» 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-Х К» при этом не выводит.