ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО

систем автоматизированного проектирования

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН
11443195.509000.047 90-ЛУ

Специальное программное обеспечение средств защиты информации от несанкционированного доступа

«АККОРД-X K»

(версия 1.0)

РУКОВОДСТВО АДМИНИСТРАТОРА

11443195.509000.047 90

Москва
2017

АННОТАЦИЯ

Настоящий документ является руководством администратора специального программного обеспечения средств защиты информации от несанкционированного доступа (СПО СЗИ НСД) «Аккорд-X K» v.1.0 (ТУ 509000-047-11443195-2008) (далее по тексту – СПО СЗИ НСД «Аккорд-X K», СПО «Аккорд-X K», «Аккорд-X K») 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 СПО «Аккорд-X K».

В документе приведены основные функции администратора безопасности информации, порядок установки и настройки СПО «Аккорд-X K», порядок установки прав доступа пользователей к информационным ресурсам, описание организации контроля работы СВТ с внедренными средствами защиты и другие сведения, необходимые для управления защитными механизмами СПО «Аккорд-X K».

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

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

Применение защитных мер СПО «Аккорд-X K» должно дополняться общими мерами технической безопасности.

СОДЕРЖАНИЕ

ПРИНЯТЫЕ ТЕРМИНЫ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Администратор БИ	- администратор службы безопасности информации
Имя_пользователя	- имя, под которым пользователь зарегистрирован в системе
Объект доступа	- под объектом доступа понимается один из перечисленных ресурсов СВТ: диск, каталог, файл, процесс (задача).
Параметры пользователя	- идентифицирующие признаки пользователя (имя, данные для идентификации, пароль) и его права по доступу к ресурсам СВТ в соответствии с его полномочиями
Пользователь	- субъект доступа к объектам (ресурсам) СВТ
ПРД	- правила (политики) разграничения доступа
Удаление пользователя	- удаление имени, под которым пользователь зарегистрирован в системе, из списка зарегистрированных пользователей в СПО «Аккорд-Х К»
Синхронизация параметров пользователя	- сопоставление 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, требуемых от пользователя, о состоянии программы и нормально завершенных действиях, сбоях в системе и др.
Идентификатор	- персональный идентификатор пользователя
Использовать идентификатор	- приложить персональный идентификатор пользователя к контактному устройству съемника информации
Число проходов при удалении	- количество проходов случайной последовательности по содержимому файла при его удалении

ВНИМАНИЕ!

Перед началом установки СПО «Аккорд-X K» рекомендуется подробно ознакомиться с эксплуатационной документацией, прежде всего с «Описанием применения» (11443195.509000.047 31) и настоящим руководством.

1 ВВЕДЕНИЕ

Специальное программное обеспечение «Аккорд-X K» v.1.0 (ТУ 509000-047-11443195-2008), далее по тексту – СПО «Аккорд-X K», СПО«Аккорд», СПО – это простое, но чрезвычайно эффективное средство, используя которое, можно надежно защитить от несанкционированного доступа информацию на СВТ, функционирующих под управлением ОС Linux, без переделки ранее приобретенных программных средств.

СПО «Аккорд-X K» 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 возможностями системы защиты информации от НСД к информационным ресурсам АС, построенной на базе СПО «Аккорд».

Не умаляя достоинств СПО «Аккорд-X K», надо сказать, что СПО «Аккорд-X K» не может решить все проблемы по созданию комплексной защиты информационных систем. Следует четко понимать, что СПО «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 СПО «Аккорд-X K» не требует изменения существующего программного обеспечения. Необходимо лишь квалифицированное применение СПО «Аккорд-X K» – правильная установка, настройка и эксплуатация в соответствии с принятыми на предприятии политиками разграничения доступа, и обеспечение организационной поддержки.

Как показывает практика довольно длительного применения СПО семейства «Аккорд»™, часто трудности заключаются в отсутствии у большинства пользователей (организаций, фирм и т.д.) установленного порядка и четких правил разграничения доступа (ПРД) 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 СПО «Аккорд-Х К», 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 над 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 СПО «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.

2 ОБЩИЕ СВЕДЕНИЯ ОБ СПО «Аккорд-X K»

2.1 Состав СПО «Аккорд-X K»

2.1.1 Общие сведения

СПО «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.

СПО «Аккорд-X K» реализовано в следующих вариантах исполнения:

- СПО «Аккорд-X K» для ОС Ubuntu 12.04 LiveCD;
- СПО «Аккорд-X K» для ОС Red Hat Enterprise Linux 5.1;
- СПО «Аккорд-X K» для ОС Red Hat Enterprise Linux 5.4;
- СПО «Аккорд-X K» для ОС Red Hat Enterprise Linux 5.7.

«Аккорд-X K» на логическом уровне состоит из следующих модулей:

- ядро защиты – программы, реализующие защитные функции «Аккорд-X K»;
- программы управления защитными функциями (настройки СПО «Аккорд-X K» в соответствии с ПРД).

В ядро защиты СПО «Аккорд-X K» входят:

- монитор разграничения доступа, выполняющий непосредственно функции защиты информации от НСД – МРД (модуль ядра Linux acx-core.ko);
- подключаемые программные модули аутентификации (PAM), взаимодействующие с монитором разграничения доступа для идентификации/аутентификации субъектов доступа, – подсистема идентификации и аутентификации (PAM-модуль pam_acx_local.so);
- утилиты, реализующие передачу файла конфигурации и базы данных пользователей в программный монитор разграничения доступа;
- утилита реализации статического контроля целостности объектов ОС (acx-integrity-controller).

Данные модули выполняют основные функции по защите информации от несанкционированного доступа.

Модули, не входящие в состав ядра защиты, либо являются вспомогательными и обеспечивают функционирование ядра защиты (например, предотвращают формирование БД неправильного формата), либо представляют

собой утилиты для удобной настройки и администрирования СПО «Аккорд-X К». В частности, к средствам администрирования СПО «Аккорд-X К» относятся следующие программы:

1) утилиты настройки СПО «Аккорд-X К» acx-admin;

2) утилиты установки ПРД пользователей acx-admin user, acx-admin group, acx-admin shadow, acx-admin acl;

3) утилиты установки ПРД процессов acx-admin process, acx-admin group, acx-admin acl;

4) утилита работы с журналами регистрации событий acx-admin log

Указанные средства не входят в ядро защиты СПО «Аккорд-X К» и сами не осуществляют никаких защитных механизмов. Строго говоря, реализация всех указанных функций защиты может осуществляться и без этих средств.

Подробное описание СПО «Аккорд-X К» см. п. 2.1.2.

2.1.2 Состав исполняемых модулей

СПО «Аккорд-X К К» поставляется в нескольких пакетах, которые имеют следующее содержание:

- пакет acx-admin - содержит утилиты администрирования СПО «Аккорд-X К» и необходимые библиотеки для работы с файлом конфигурации и БД (libacx-db), журналом безопасности (libacx-log);
- пакет acx-core - содержит модуль acx-core.ko (МРД), библиотеку и модули взаимодействия с МРД (libacx-core, acx-config-send, acx-db-send), модуль статического контроля целостности (acx-integrity-controller), набор PAM-модулей (pam_acx_local.so, pam_acx_marsh.so pam), скрипты распаковки и упаковки образа initrd для возможности установки МРД. Данный пакет содержит основную часть ядра защиты Аккорд-X К (за исключением подсистемы контроля печати);
- пакет acx-print - содержит библиотеку взаимодействия МРД и модуля контроля печати и непосредственно сам модуль печати, относящийся к ядру защиты СПО «Аккорд-X К».

Модуль acx-core.ko (МРД) является ключевым модулем в архитектуре Аккорд-X К - это ядро СПО Аккорд-X К, выполненное в виде загружаемого модуля ядра (LKM). Этот модуль реализует большую часть функций защиты:

- реализация дискреционных политик разграничения доступа и контроля доступа на основе иерархических меток;
- динамический контроль целостности;
- очистка остаточной информации на внешних носителях;
- регистрация системных событий в журнале безопасности.

Утилиты acx-config-send, acx-db-send являются средством получения МРД, необходимых данных для корректной реализации ПРД, заданных Администратором с помощью утилит администрирования acx-admin*.

Модули PAM (pam_acx_local.so, pam_acx_marsh.so) представляют собой динамически загружаемые библиотеки, реализующие механизм идентификации пользователя и взаимодействия с МРД для его аутентификации. Само решение о доступе принимается МРД acx-core.ko, на основании полученных от PAM-модуля данных и их соответствию данным в собственной БД. PAM-модули отвечают за запрос входных данных от пользователя и процедуру регистрации/блокирования пользователя в ОС на основании ответа от МРД, при этом использовать их можно как для штатных сценариев идентификации/аутентификации в ОС (для утилит login, gdm, kdm и т.п.), так и для других приложений (вообще говоря, для любых).

Модуль acx-integrity-controller реализует функции статического контроля целостности файлов/исполняемых модулей. МРД в ходе загрузки ОС и в момент входа пользователя в систему инициирует выполнение этого модуля для статического контроля (динамический контроль реализован самим МРД).

2.2 Назначение СПО «Аккорд-Х К»

СПО «Аккорд-Х К» предназначено для защиты от несанкционированного доступа к информации, обрабатываемой и хранимой в СВТ и АС, по требованиям Системы сертификации средств защиты информации № РОСС RU.0001.01.БИ00[1].

СПО «Аккорд-Х К» 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.

1 Данные об уровнях защищенности, обеспечиваемых СПО «Аккорд-Х К», приведены в табл.1. ТУ 509000.047-11443195-2011

2.3 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 пространства для установки СПО – не менее 128 Мб.

2.4 Организационные меры, необходимые для применения СПО «Аккорд-Х К»

Для эффективного применения СПО «Аккорд-Х К» и поддержания необходимого уровня защищенности СВТ (РС) и информационных ресурсов АС **необходимо**:

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

Прием в эксплуатацию СПО «Аккорд-Х К» оформляется актом в установленном порядке, в формуляре на СПО «Аккорд-Х К» администратором БИ делается соответствующая отметка.

3 СОДЕРЖАНИЕ РАБОТЫ АДМИНИСТРАТОРА БИ ПО ПРИМЕНЕНИЮ СПО «АККОРД-Х К»

Основное содержание работы администратора БИ по применению СПО «Аккорд» составляют следующие мероприятия:

- планирование применения СПО «Аккорд-Х К» (подробнее см. раздел **Ошибка! Источник ссылки не найден.**);
- организация установки СПО «Аккорд-Х К» и настройка его защитных средств в соответствии с установленными политиками разграничения доступа (подробнее см. раздел 4);
- эксплуатация СВТ с внедренным СПО «Аккорд-Х К», в т.ч., организация контроля над правильностью применения защитных механизмов СПО «Аккорд-Х К» (подробнее см. раздел 5);
- снятие защиты (подробнее см. раздел 6).

4 УСТАНОВКА И НАСТРОЙКА СПО «АККОРД-Х К»

4.1 Общие сведения

Администратор БИ организует установку и настройку СПО «Аккорд», исходя из принятой в организации политики информационной безопасности, и осуществляет контроль качества ее выполнения.

В настоящем разделе рассматривается порядок настройки защитных механизмов СПО в соответствии с правилами разграничения доступа 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 СПО «Аккорд-Х К») организационно-распорядительными документами.

Полномочия пользователей по доступу к ресурсам АС (СВТ) назначаются путем соответствующей настройки:

- средств идентификации и аутентификации пользователей, с учетом необходимой длины пароля;
- 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 СПО «Аккорд-Х К»;
- механизмов управления стандартными процедурами печати, процедурами ввода/вывода на отчуждаемые носители информации.

4.2 Порядок установки и настройки 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» и состоит из следующих этапов:

1. установка СПО разграничения доступа (подробнее см. подраздел 4.3.1);

2. настройка защитных механизмов СПО «Аккорд-Х К» (в т.ч. назначение ПРД для пользователей в соответствии с политикой информационной безопасности) и активизация подсистемы разграничения доступа к ресурсам ПЭВМ (подробнее см. подраздел 4.4);

3. реализация организационных мер защиты, рекомендованных в эксплуатационной документации на СПО «Аккорд-Х К».

4.3 Установка СПО «Аккорд-Х К»

4.3.1 Установка СПО разграничения доступа«Аккорд-Х К»

Перед эксплуатацией СПО «Аккорд-Х К» необходимо выполнить процедуру установки СПО разграничения доступа в ОС.

Администратор БИ устанавливает СПО с дистрибутивного носителя, входящего в комплект поставки СПО «Аккорд-Х».

Для rpm-based дистрибутивов это можно сделать с помощью следующих команд:

ВНИМАНИЕ!

При установке СПО «Аккорд-Х К» на deb-based дистрибутивы ОС Linux (Ubuntu, Debian и другие) следует вместо команды «rpm -ivh ...» использовать «dpkg -i ...».

```
# rpm -ivh acx-admin-1.0-1.i686.rpm
# rpm -ivh acx-core-0.1-1.i686.rpm
# rpm -ivh acx-tmid-usb-1.0-1.i686.rpm
... (здесь могут быть прочие пакеты для поддержки идентификаторов)
# rpm -ivh acx-amdz-1.0-1.rpm
```

ВНИМАНИЕ!

Перед установкой пакета acx-tmid-tokens необходимо вручную скопировать следующие отдельные модули, не входящие в какие-либо пакеты:

cp libccid_dev.so /usr/lib/

cp tmid-etoken_pro_java-apdu.so /usr/lib/

cp pam_acx_marsh.so /lib/security

В операционных системах семейства RHEL после копирования указанных модулей при установке пакета acx-tmid-tokens может возникнуть ошибка с неразрешенными зависимостями (libccid_dev.so). Во избежание этого пакет acx-tmid-tokens следует устанавливать следующим образом:

rpm -ivh --nodeps acx-tmid-tokens-1.1-0.i686.rpm

ВНИМАНИЕ!

При установке ряда rpm-пакетов может возникнуть предупреждение о том, что в настройках ОС необходимо разрешить загрузку неподписанных драйверов и модулей ядра (например, в /etc/modprobe.d/unsupported-modules параметру allow_unsupported_modules установить значение 1).

4.4 Настройка СПО разграничения доступа

4.4.1 Начальная конфигурация СПО «Аккорд-Х К»

После выполнения процесса установки СПО разграничения доступа (п.4.3.1) необходимо провести начальную конфигурацию СПО «Аккорд-Х К» с помощью утилиты *acx-config* (входит в состав пакета *acx-admin - acx-admin config*). Для автоконфигурирования СПО «Аккорд-Х К» следует выполнить команду (см. рисунок 1):

```
# acx-config create
```

```
[root@localnost ~]# acx-admin config create
[root@localhost ~]# acx-admin config show
common:
        db-path:              /etc/accordx/db.json
        log-dir-path:         /var/log/accordx/
salt:
        salt-prefix:          $1$
        salt-size:            8
        salt-end-symbol:      $
company:
        company-name:         ""
        company-phone:        ""
acx-core flags:
        permissive-acl:       true
        discr-acl:            false
        mand-acl:             false
        star-property:        true
        soft-mode:            true
        mpl:                  false
        icl:                  false
        print-control:        false
        memory-cleaning:      false

        default-log-level:    err
clearance-transcript:
        0 - "public"
        1 - "confidential"
        2 - "secret"
        3 - "top secret"
        4 - "special importance"
autentication settings:
        authentication-type: local
        pam-retries:          10
        block-multilogin:     false
        password-length:      8
```

Рисунок 1 - Создание файла конфигурации, вывод созданного файла конфигурации «Аккорд-X K»

В результате выполнения приведенной команды в /etc/accordx/acx-config.json создастся конфигурационный файл для СПО «Аккорд-X» вида:

```
common:
        db-path:  /etc/accordx/db.json
        log-dir-path:  /var/log/accordx/
salt:
        salt-prefix:   $6$
        salt-size:     8
        salt-end-symbol:    $
```

```
company:
          company-name:  ""
          company-phone: ""
acx-core flags:
     permissive-acl:     true
          discr-acl:          false
          mand-acl:           false
          star-property:      true
          soft-mode:          true
          mpl:                false
          icl:                false
          print-control:      false
          memory-cleaning:    false
          default-log-level:  err

clearance-transcript:
          0 - "public"
          1 - "confidential"
          2 - "secret"
          3 - "top secret"
          4 - "special importance"

autentication settings:
          authentication-type: local
          pam-retries:         10
          block-multilogin:    false
          password-length:     8
```

где:

1) log-dir-path –путь для создания журналов;

2) блок acx-core flags используется для выполнения настроек ядра защиты СПО «Аккорд-Х К». Параметры блока:

- permissive-acl – включить разрешительные ПРД;
- discr-acl – включить дискреционную политику разграничения доступа;
- mand-acl – включить политику разграничения доступа на основе иерархических меток;
- star-property – включить правило запрета “писать вниз” в политике разграничения доступа на основе иерархических меток;
- soft-mode – включить мягкий режим;
- mpl – включить контроль точек монтирования;
- icl – включить контроль целостности;
- print-control включить контроль печати;
- memory-cleaning включить очистку оперативной памяти;
- default-log-level уровень детальности журнала событий;

3) clearance-transcript – используется для задания соответствия между строками и иерархическими метками ;

4) authentication setting включает новые опции:

- password-length (минимальная длина пароля для всех пользователей):
- block-multilogin (запрещать возможность создания множественных сессий одного и того же пользователя);
- pam-retries (максимальное количество попыток сделать login перед блокировкой);
- authentication-type (тип аутентификации – локальная, с пробросом пользователя из контроллера (passthrough), удаленная).

4.4.2 Создание базы данных пользователей

Далее с помощью утилиты acx-admin (*acx-admin db create)* следует создать базу данных (БД) пользователей (подробнее см. рисунок 2). Если на предыдущем шаге был корректно создан конфигурационный файл, то на данном шаге можно использовать опцию –c для создания БД со стандартными учетными записями, необходимыми далее: # acx-admin db create -c

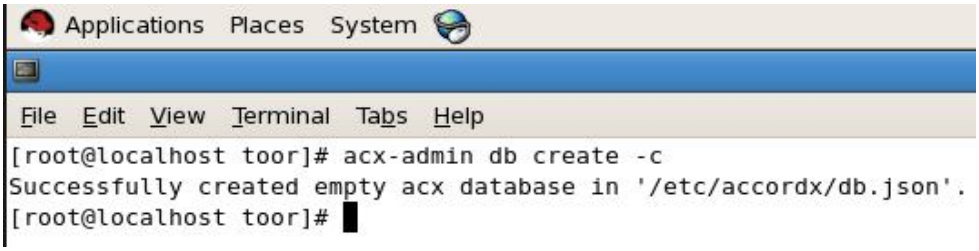

Рисунок 2 – Создание базы данных пользователей на основе конфигурационного файла

В результате выполнения приведенной команды в /etc/accordx/db.json создается файл базы данных пользователей.

Можно выполнить просмотр БД, использовав опцию –v – показать подробный вывод (рисунок 3):

```
# acx-admin db show -v
```

```
[root@localhost accordx]# acx-admin db show -v
Account database version: 1.1
Accounts: 2 group(s), 1 user(s), 1 shadow(s), 0 process(es)
        group "default_shadow"(shadow), 1 member(s)
        group "default_user"(user), 1 member(s)
        Mandate ACL: 0 rule(s)
        Global static ICL: 0 object(s)
        Global dynamic ICL: 0 object(s)
```

Рисунок 3 –Просмотр параметров БД

Чтобы в процессе дальнейшего функционирования СПО «Аккорд-Х К» можно было выполнить вход в ОС в качестве Администратора ИБ

(суперпользователя; пользователя root), после создания базы данных пользователей ему необходимо назначить данные для идентификации и аутентификации (данную процедуру необходимо выполнить потому, что при создании БД использовалась опция автосоздания нужных по умолчанию пользователей, и, следовательно, данные для идентификации и аутентификации для пользователя root еще не заданы). См. рисунок 4.

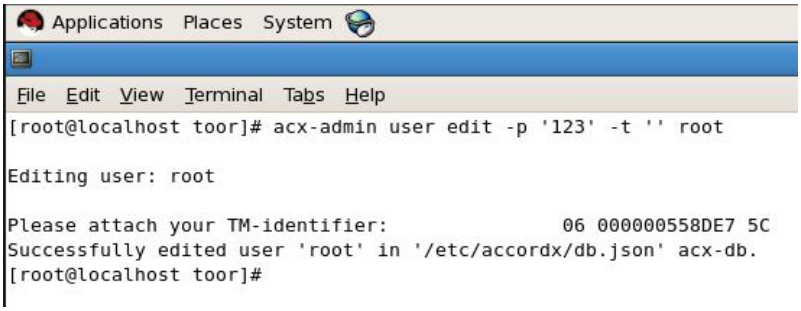

Рисунок 4 - Назначение данных для идентификации и аутентификации для пользователя root

4.4.3 Создание групп пользователей

Чтобы создать группу пользователей, необходимо запустить утилиту acx-admin group (`acx-db-group`) - подробнее см. рисунок 5:

```
# acx-admin group [add|delete] GROUPNAME
```

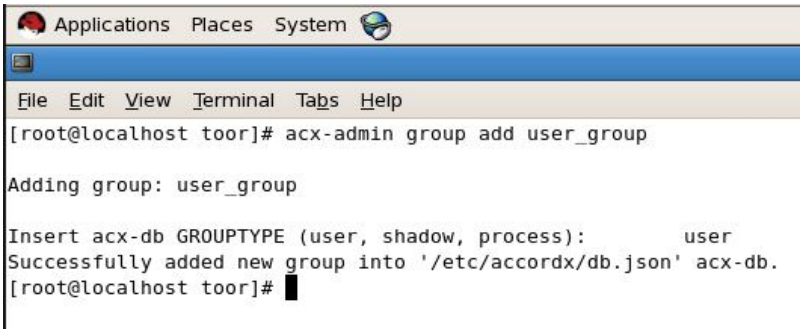

Рисунок 5 – Создание группы пользователей

На данный момент группирование пользователей не оказывает влияния на общую работу СПО «Аккорд-Х К» – группы используются для удобства. Однако необходимо учитывать, что для корректной работы СПО «Аккорд-Х К» должны выполняться следующие условия:

в БД обязательно должна быть зарегистрирована учетная запись пользователя типа shadow (и, соответственно, группа типа shadow) с именем "root", uid=0 и максимальными дискреционными ПРД на все объекты файловой системы (в случае применения команды '#acx-admin db create -c' такая учетная запись будет создана автоматически). Данная учетная запись используется в мониторе разграничения доступа СПО «Аккорд-Х К» на раннем этапе загрузки ОС (т.е. до появления в системе реального пользователя), в соответствии с

этим ПРД для этой учетной записи редактировать не рекомендуется, т.к. это может привести к ошибке в загрузке ОС и/или kernel panic.

в БД обязательно должна быть зарегистрирована учетная запись пользователя типа user (и, соответственно, группа типа user) с именем "root" и uid=0. Данная учетная запись в некоторых ОС может использоваться на позднем этапе загрузки ОС. В рамках самой ОС эта учетная запись соответствует учетной записи суперпользователя (root). Если при настройке СПО «Аккорд-Х К» не планируется каким-либо образом ограничивать учетную запись суперпользователя, дискреционные ПРД для этой учетной записи лучше задать такими же, как и для учетной записи пользователя shadow с именем root (т.е. максимальные ПРД для всех объектов файловой системы, максимальный уровень конфиденциальности). Дополнительно для этой учетной записи необходимо задать данные для идентификации и аутентификации (см. рисунок 5).

4.4.4 Создание учетных записей пользователей

Для создания учетных записей пользователей необходимо запустить утилиту *acx-admin user* [add|edit|delete]. Данные учетные записи в дальнейшем будут использоваться для реальных пользователей системы.

При создании пользователей необходимо учесть тот факт, что в ходе выполнения процедуры входа в ОС от имени пользователя в системе будет выполняться ряд утилит, а также использоваться большое количество библиотек. Настоятельно рекомендуется первоначально задать пользователю максимальные права и запустить систему в «мягком» режиме. Затем из лога работы пользователя можно будет сформировать более точные ПРД с помощью утилиты *acx-admin-log* (командой # acx-admin log makerights ...).

Создадим, например, обычного пользователя с именем toor.

```
acx-admin user add -w '' -a user_group toor
```

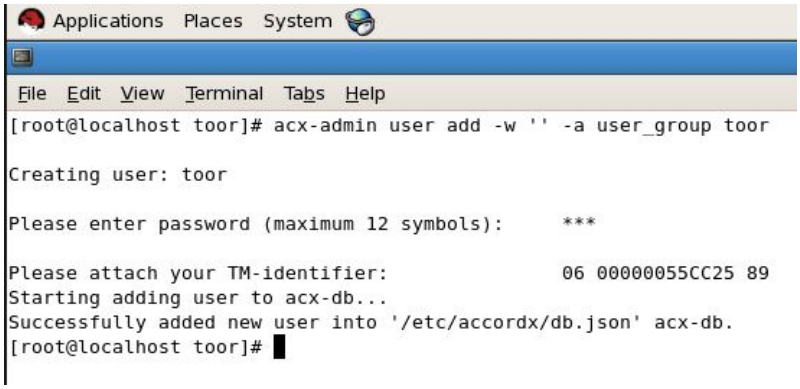

Рисунок 6 – Создание обычного пользователя с именем toor

После выполнения описанной последовательности действий пользователь с именем toor появляется в базе данных пользователей СПО «Аккорд-Х К».

```
[root@localhost accordx]# acx-admin user show toor
toor tmid=[06 0000004F31AA 2E] xid.tmdevice=[394AD69AD84419DC] xid.accordle=[394AD69AD84419DCFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF] uid=[1500]
        Working hours:

        Capabilities: set_time
        Settings:
        Mandatory level: 0
        Blocked: false
        ACL: 1 rule(s)
        Static ICL: 0 object(s)
        Dynamic ICL: 0 object(s)
[root@localhost accordx]#
```

Рисунок 7 – Просмотр параметров пользователя

В Н И М А Н И Е !

При создании или редактировании пользователей необходимо удостовериться, что uid реальных пользователей, создаваемых в БД «Аккорд-Х К», совпадают со значениями из файла /etc/passwd. Иначе произвести операцию login данным пользователем не получится. Если пользователь, создаваемый в «Аккорд-Х К» уже существует в ОС, то необходимо указать его реальный uid с помощью опции -u – например, «acx-admin user add -u 1000 USERNAME».

Необходимо отметить, что все операции по формированию или просмотру БД пользователей требуется выполнять с помощью утилит acx-admin-*. Это связано с тем, что ручное создание/редактирование данных в файле БД может привести к тому, что в монитор разграничения доступа будет загружена БД неправильного формата (что с большой вероятностью приведет к панике ядра на раннем этапе загрузки ОС). Все приведенные в документе демонстрации файлов БД или конфигурации призваны сформировать понимание принципов настройки СПО «Аккорд-Х К» у Администратора БИ - на практике же для просмотра результатов выполнения той или иной команды рекомендуем использовать утилиты из состава acx-admin-* (например, acx-admin user show для просмотра информации по пользователям и т.п. - см. Приложение 2).

4.4.5 Задание дискреционных прав разграничения доступа

Рассмотрим вопрос задания ПРД для созданных пользователей «Аккорд-Х К».

Итак, после успешного выполнения установки и первичной настройки СПО «Аккорд-Х К» (см. п. 4.4.1, 4.4.2, 4.4.3, 4.4.4) необходимо задать дискреционные политики разграничения доступа созданным пользователям с помощью утилиты *acx-admin acl*.

В СПО «Аккорд-Х К» дискреционные правила разграничения доступа устанавливаются присвоением объектам доступа атрибутов доступа. Установленный атрибут означает, что определяемая атрибутом операция может

выполняться над данным объектом. В дискреционной политике разграничения доступа доступны 12 атрибутов:

R - открытие объекта на чтение;

W - открытие объекта на запись;

X - открытие объекта на выполнение;

O - подмена атрибута R атрибутами RW на этапе открытия объекта;

C - создание объекта;

D - удаление объекта;

N - переименование объекта;

L - создание жесткой ссылки для объекта

M - создание каталога;

E - удаление каталога;

n – переименование каталога;

G - переход в каталог.

Различные атрибуты для каталогов можно задавать без рекурсии, рекурсивно на 1 подкаталог вниз или рекурсивно на все подкаталоги указанного каталога (при этом в БД это отображается в виде различных окончаний у объектов контроля - /, /* или /** соответственно).

Типы наследования прав доступа для содержимого контейнеров:

0 - Нет наследования

1 - Наследование подкаталогами атрибутов родительского каталога только на один уровень вложенности

S - Рекурсивное наследование подкаталогами атрибутов родительского каталога.

Пример: Демонстрация задания дискреционной политики безопасности

Создадим в ОС 4 каталога - /home/toor/nocd, /home/toor/noread, /home/toor/nowrite, /home/toor/noexec и для пользователя toor зададим соответствующие ограничения на них (нельзя перейти в каталог, нельзя читать, нельзя писать, нельзя выполнять соответственно; см. рисунок 8).

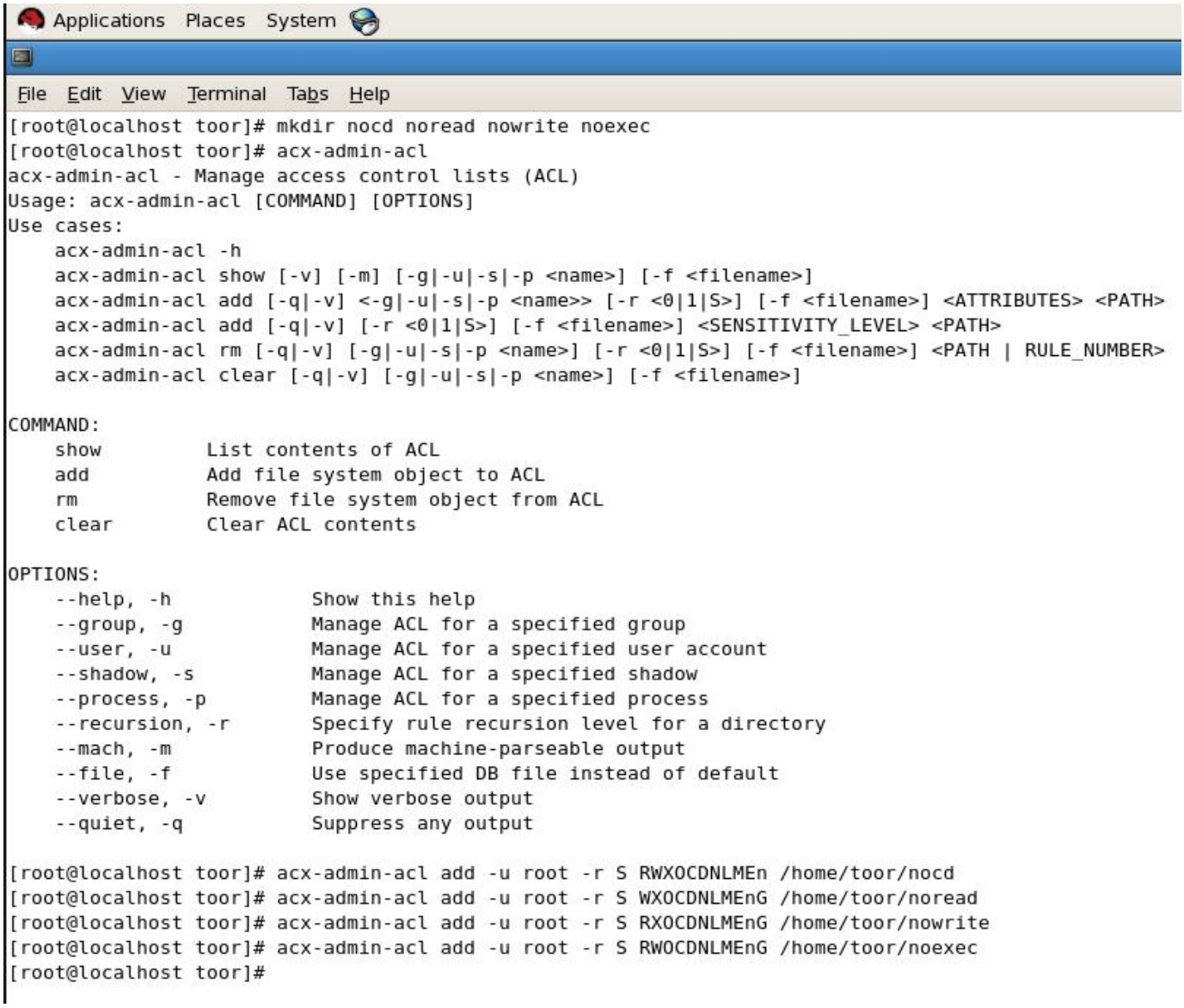

Рисунок 8 – Задание дискреционной политики безопасности

Таким образом, созданные правила разграничения доступа в БД «Аккорд-X K» должны иметь следующий вид:

```
"acl":  [["/**", "RWXOCDNLMEnG"], ["/home/toor/nocd/**",
"RWXOCDNLMEn"], ["/home/toor/noexec/**", "RWOCDNLMEnG"],
["/home/toor/noread/**", "WXOCDNLMEnG"], ["/home/toor/nowrite/**",
"RXOCDNLHEnG"]]
```

4.4.6 Задание меток и уровней доступа

Задать иерархические метки для объектов файловой системы и уровни доступа для пользователей можно с использованием утилиты acx-admin acl. В «Аккорд-X K» поддерживаются метки от 0 до 15. При этом уровни доступа необходимо выставить для всех пользователей системы (параметр clearance), а

уровни конфиденциальности - для каждого объекта (уровни конфиденциальности будут глобальными для всей системы). Также необходимо помнить, что для начала своей работы механизм разграничения доступа на основе иерархических меток должен быть включен в файле конфигурации (выше в первичном конфигурировании был включен только дискреционный механизм).

Данный шаг рекомендуется пропустить, пока в системе не будет корректно работать дискреционная политика разграничения доступа (либо автоматически задать метки из лога работы в "мягком" режиме).

В Н И М А Н И Е !

При настройке различных политик разграничения доступа необходимо понимать, что после загрузки монитора разграничения доступа БД пользователей начнет «защищать сама себя». Поэтому на этапах 4.4.5 и 4.4.6 необходимо четко разграничить, каким пользователям будут доступны на чтение/редактирование сам файл БД, а также все утилиты администрирования из пакета *acx-admin* (/bin/acx-admin-*).

4.4.7 Создание списков контроля целостности

Создание списков контроля целостности (СКЦ) выполняется с помощью утилиты *acx-admin icl*.

Данный пункт, как и предыдущие два, можно пропустить и выполнить только после настройки «Аккорд-X K» с «пустой» БД.

Существует 2 типа контроля целостности – динамический и статический.

4.4.7.1 Динамический контроль целостности

Динамический контроль целостности осуществляется в мониторе разграничения доступа при запуске на исполнение указанных объектов (объекты необходимо указывать в динамическом списке контроля целостности глобально для всей БД, а не для конкретного пользователя - db->dynamic_icl).

Пример. Демонстрация заполнения списка динамического контроля целостности.

Создадим бинарный файл (выводящий в консоль «ok») и занесем его в динамический список контроля целостности (рисунок 9).

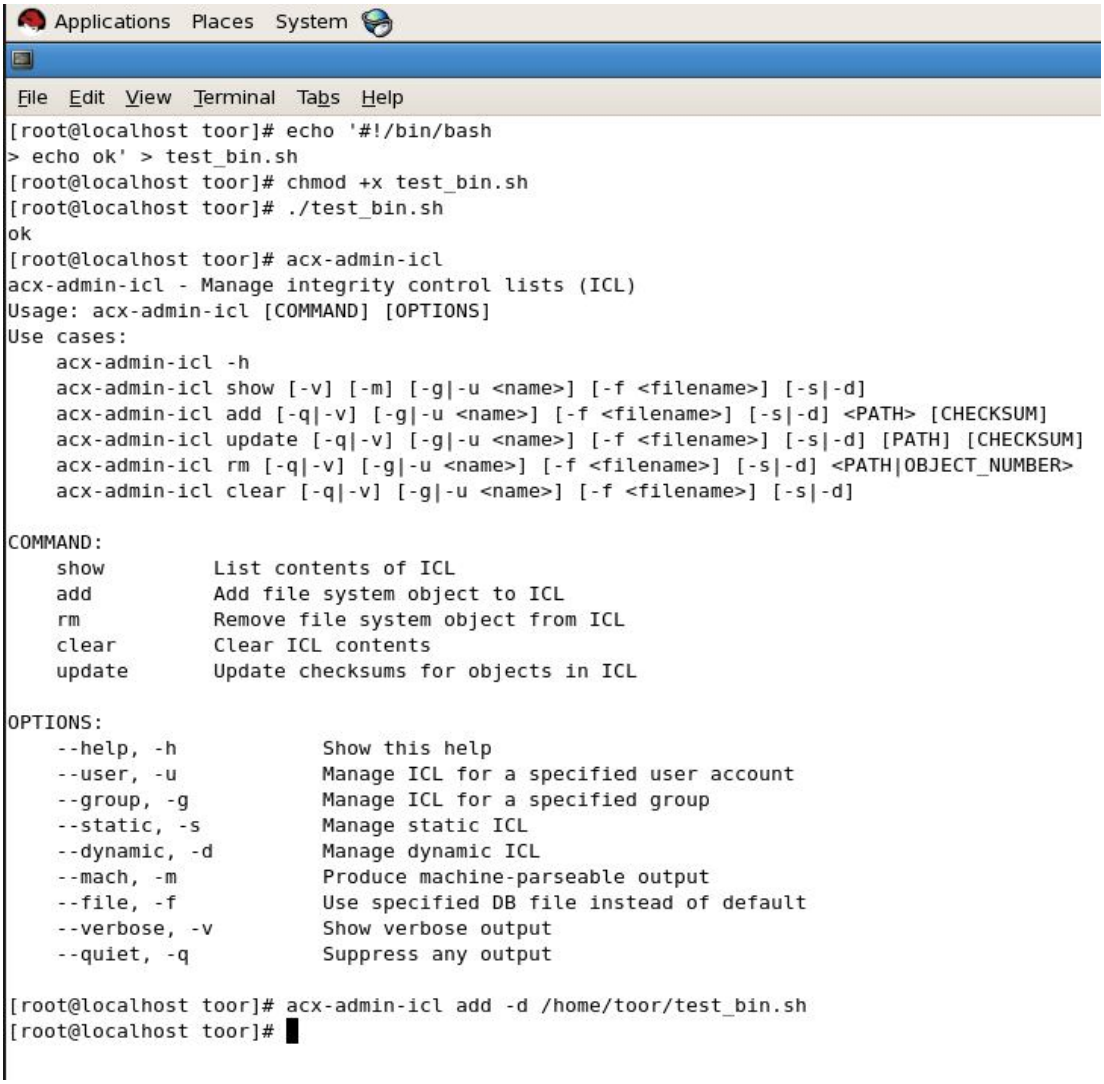

Рисунок 9 – Создание и занесение в динамический СКЦ бинарного файла

Только что добавленный объект в динамическом СКЦ выглядит следующим образом:

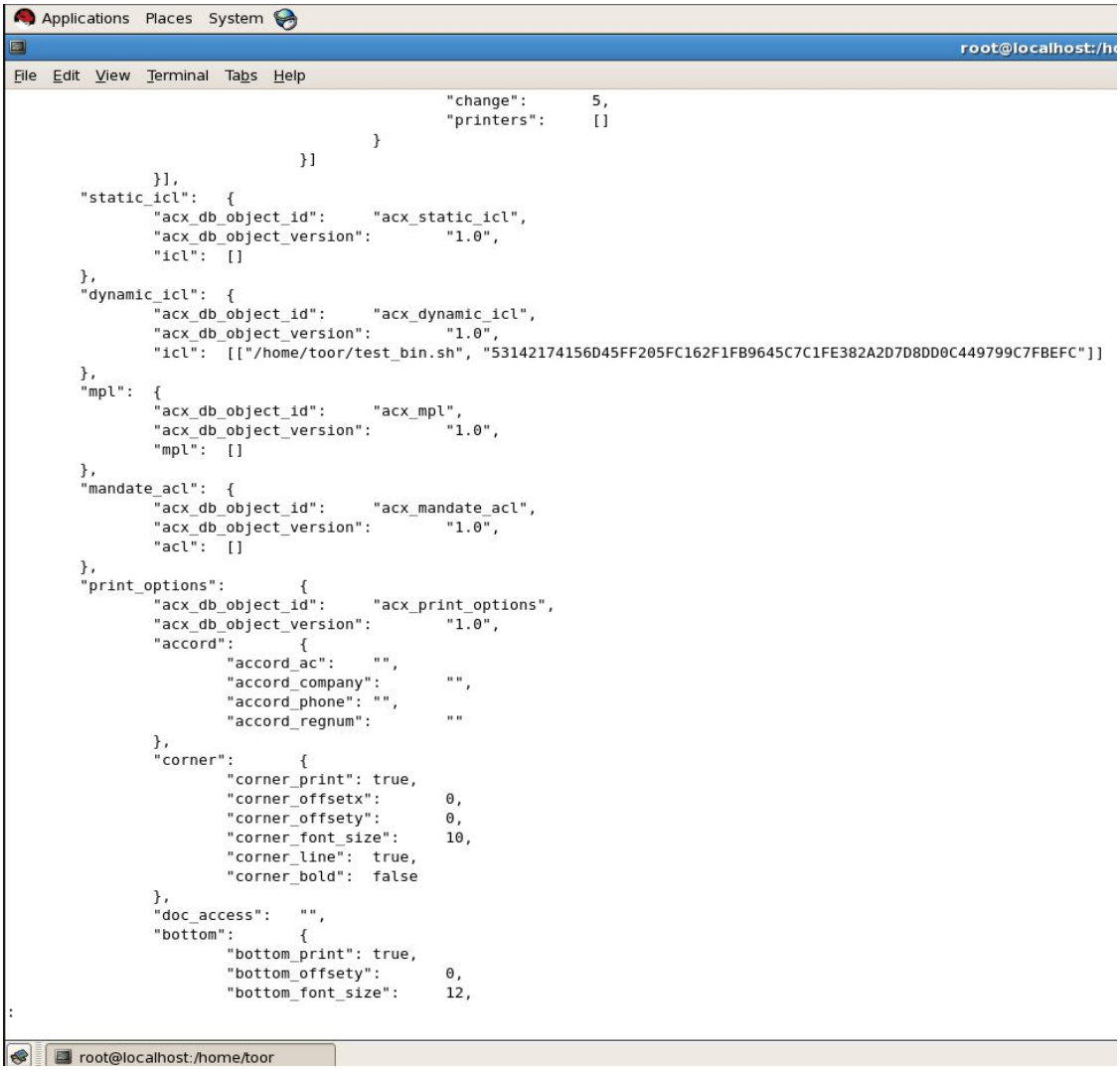

Рисунок 10 – Демонстрация добавленного в динамический СКЦ объекта

4.4.7.2 Статический контроль целостности

Статический контроль целостности осуществляет контроль целостности любых файлов в тот момент, когда запускается утилита *acx-integrity-controller/acx-integrity-controller-db*. Таким образом, для проведения контроля целостности системных файлов ОС, можно добавить выполнение этой утилиты в скрипт инициализации (/etc/rc.sysinit и аналоги), например, так:

```
#################################################################
echo "Starting AccordX integrity control scan..."
#wait 3
/bin/acx-integrity-controller-db -v /etc/accordx/db.json
if [ $? -ne 0 ]; then
        echo "Fount integrity error - you should call your system
administrator to check what happend!!!"
        echo -n "Do you want to proceed loading anyway? [y/n] "
```

```
        read answer
        if [ $answer = "y" ]; then
                echo "Continue loading operating system..."
        else
#               panic "AccordX found integrity errors. Please call
your system administrator."
                echo "Rebooting due to integrity check errors..."
                reboot
        fi
else
        echo "Integrity check finished successfully. Continue loading
operating system..."
fi
#####################################################################
```

Важно, чтобы статический контроль целостности выполнялся сразу после перемонтирования root filesystem на запись в /. Объекты для статического СКЦ необходимо добавлять для БД - т.е. в db->static_icl.

Однако рекомендуется осуществлять статический контроль целостности ядром СПО «Аккорд-Х К». Для включения статического контроля целостности PAM-модулю (pam_acx_local.so или другому, см. 4.5.1) нужно дописать опцию icl через пробел:

```
auth …    pam_acx_local.so icl
```

В Н И М А Н И Е !

При формировании прав разграничения доступа и списков контроля целостности необходимо указывать полные абсолютные пути до объектов доступа.

В Н И М А Н И Е !

Политики разграничения доступа сначала следует настраивать «наоборот», т.е. вначале дать каждому пользователю права на все действия с учетом прав доступа ОС (для дискреционной политики – «acx-admin acl add -u USER -r S RWXOCDNLMEnG /»), а затем ограничивать доступ к конкретным объектам («acx-admin acl add -u USER -r S WXOCDNLMEnG /home/user/noread/»). Такой порядок задания прав доступа СПО «Аккорд-Х К» более предпочтителен, т.к. во время загрузки ОС и логина пользователя операционная система осуществляет доступ к определенным объектам файловой системы для создания необходимого окружения, запуска определенных процессов и т.п. (этих объектов может быть достаточно много).

В Н И М А Н И Е !

Существует также возможность задания изначально разрешительных правил разграничения доступа (когда изначально всем пользователям в

системе всё разрешено, а не запрещено). Для задания разрешительных ПРД в файле конфигурации СПО «Аккорд-Х К» существует опция permissive-acl.

4.5 Настройка корректного разграничения доступа

4.5.1 PAM-модуль

Для корректного входа в ОС пользователей в систему и регистрации их в мониторе разграничения доступа необходимо корректным образом настроить PAM в ОС Linux. Только при выполнении этого условия ядро СПО «Аккорд-Х К» будет обеспечивать корректное разграничение доступа для пользователей и контроль целостности объектов файловой системы.

Монитор разграничения доступа обрабатывает все события регистрации пользователя в ОС за счет PAM-модуля СПО «Аккорд-Х К», который необходимо описать в правилах PAM для утилит, ответственных за логин в ОС. Данный PAM-модуль осуществляет взаимодействие с монитором разграничения доступа для идентификации и аутентификации пользователя в самом мониторе, а не в ОС (запрос данных для идентификации и аутентификации осуществляет PAM, проверку производных от них значений осуществляет сам монитор по своей БД).

Обращаем Ваше внимание, что в различных версиях и дистрибутивах ОС Linux конкретные сценарии и названия PAM-модулей могут отличаться, в связи с чем в данном описании мы можем лишь показать принцип, в соответствии с которым необходимо настраивать PAM.

PAM в ОС Linux представляет собой набор модулей аутентификации, которые физически располагаются в /lib/security (при установке пакета *acx-core* в /lib/security, например, добавляется PAM-модуль *pam_acx_local.so*). В каталоге с настройками PAM (/etc/pam.d/) располагаются сценарии аутентификации для различных приложений. Как правило, для корректной работы «Аккорд-Х К» необходимо изменить сценарии для login, gdm/kdm/xdm, su, sudo. Однако при этом стоит более детально изучить каталог /etc/pam.d на предмет других сценариев, работа которых при этом может некорректно контролироваться с помощью «Аккорд-Х К».

Рассмотрим настройку PAM на следующем примере:

а) для утилиты *login* (/etc/pam.d/login) сценарий имеет следующую строчку (рисунок 11):

```
auth       include  system-auth
...
```

Таким образом для него первой строкой подключается сценарий-шаблон system-auth (такая вложенность шаблонов в некоторых ОС может быть длиннее чем 2), т.е. для того чтобы увидеть реальную последовательность PAM-модулей

для осуществления входа в ОС с консоли, следует смотреть файл /etc/pam.d/system_auth.

Рисунок 11 – Утилита login

б) сценарий *system-auth* (/etc/pam.d/system_auth) содержит следующие строки (рисунок 12):

```
auth        required        pam_env.so
auth        sufficient      pam_unix.so nullok try_first_pass
auth        requisite       pam_succeed_if.so uid >= 500 quiet
...             ...             ...
```

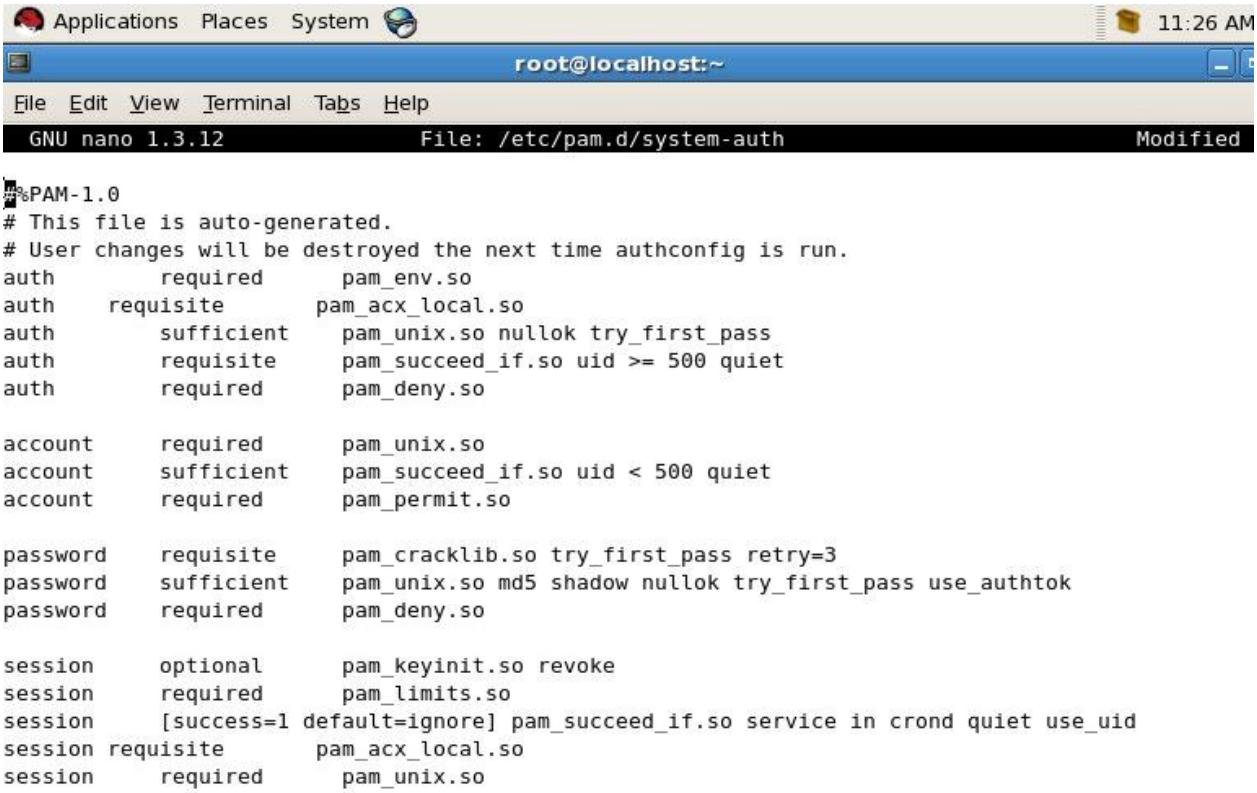

Рисунок 12 – Сценарий system-auth

В данном случае нас интересует PAM-модуль *pam_unix.so* (данный модуль, как правило, имеет имя *pam_unix.so*, однако на некоторых ОС оно может отличаться), который выполняет запрос пароля и его проверку в /etc/passwd | /etc/shadow.

в) в /etc/pam.d/system_auth зададим наш PAM-модуль *pam_acx_local.so* вместо стандартного модуля, осуществляющего проверку логина/пароля пользователя в ОС (*pam_unix.so*). В итоге содержимое *system-auth* имеет следующий вид:

```
auth        required        pam_env.so
auth        requisite       pam_acx_local.so
auth        sufficient      pam_unix.so nullok try_first_pass
auth        requisite       pam_succeed_if.so uid >= 500 quiet
```

В Н И М А Н И Е !

Для работы комплекса без аппаратных идентификаторов здесь и далее следует вместо pam_acx_local.so аналогичным образом прописывать pam_acx_marsh.so. При этом без аппаратных идентификаторов в систему могут входить только пользователи root (необходимо предварительно назначить ему идентификатор в виде строки «AA 123456789000 CD») или user (соответственно, «AA 123456789000 CC»).

Для других учетных записей можно использовать аппаратные идентификаторы (они запрашиваются только первые 2 секунды при входе в ОС, после этого войти в систему можно только под учетными записями

root/user. В крайнем случае можно выполнить ввод ошибочных данных, чтобы процесс идентификации/аутентификации начался заново).

г) как правило, при изменении сценариев-шаблонов оказывается воздействие на прочие сценарии. В приведенном примере вместе с *login* сценарий аутентификации будет изменен и для утилит *su/sudo* (т.к. мы изменили сценарий *system-auth*, который тоже используется в *su/sudo* на нашей системе) – чего, вообще говоря, не требуется. Таким образом, желательно создать копию *system-auth* (*system-auth.acx*), использовать этот шаблон в сценарии *login* и изменять уже его, чтобы быть уверенным, в том, что сценарий изменится только для нужной утилиты.

д) аналогичным образом можно настроить сценарии для GUI – *gdm/kdm/xdm*, а также прочих утилит.

Применяя описанные выше рассуждения для секции auth, аналогично PAM-модуль «Аккорд-X К» необходимо прописать для секции session:

```
...
session    requisite      pam_acx_local.so
session    required       pam_unix.so
```

Необходимо помнить, что при указанной выше настройке PAM нужно удостовериться в том, что пароли, заданные в «Аккорд-X К», соответствуют паролям пользователей ОС.

PAM-модули «Аккорд-X К» можно использовать для блокировки сессии пользователей при включении штатного хранителя экрана в ОС Linux. Для этого PAM-модуль нужно аналогичным образом прописать для приложений типа gnome-screensaver или аналогичных (в зависимости от установленного приложения-скринсейвера). Однако необходимо иметь ввиду, что использование опции блокировки мультилогина пользователей в ядре защиты «Аккорд-X К» совместно с указанной выше возможностью недопустимо (разблокировать сессию в таком случае сможет только пользователь root).

В Н И М А Н И Е !

Для корректной работы su/sudo (для смены пользователей в т.ч. в «Аккорд-X К») необходимо внести в конец файла /etc/sudoers следующую строку «Defaults timestamp_timeout=0» (в данном случае введенный пароль для sudo запоминаться не будет: каждый раз потребуется аутентифицировать пользователя), а в файле /etc/pam.d/su необходимо закомментировать строку с «auth sufficient pam_rootok.so» (т.е. запрашивать пароль при использовании su в т.ч. и у пользователя root).

В Н И М А Н И Е !

Настройку PAM-модуля рекомендуется осуществлять на самом последнем шаге, уже после того, как модуль ядра загружается и корректно работает (без аутентификации средствами *pam_acx_local.so* система будет работать с правами shadow root из db.json). При тестировании работы PAM желательно всегда иметь открытую консоль с правами root (чтобы поменять сценарии PAM

обратно), иначе в систему будет невозможно зайти. Если же сценарии PAM обратно поменять уже нельзя – остается возможность загрузки в single user mode (если она не отключена в ОС) или, например, с live-cd.

4.5.2 Настройка запуска монитора разграничения доступа

Необходимо обеспечить запуск монитора разграничения доступа на раннем этапе загрузки системы (т.е. из файла *initrd*). На данный момент данная настройка осуществляется только в ручном режиме, т.к. для различных ОС состав и формат initrd может сильно отличаться. Для осуществления этого шага необходимо выполнить следующую последовательность действий:

а) перейти в каталог /boot (убедиться, что раздел boot примонтирован, если нет – примонтировать его) и скопировать текущий образ начальной загрузки initrd (рисунок 13):

```
# cd /boot
# cp [current_initrd] initrd
```

б) распаковать созданную копию initrd с помощью скрипта из пакета *acx-core* (рисунок 13):

```
# ./initrd_unpack.sh
```

в) скопировать файл модуля ядра защиты (acx-core.ko) и необходимые утилиты (acx-db-send, acx-config-send, acx-license-send) в распакованный образ initrd (.initrd-tmp/fs) (рисунок 13):

```
# cp /lib/acx-core.ko .initrd-tmp/fs/lib/
# cp /bin/acx-db-send .initrd-tmp/fs/bin
# cp /bin/acx-config-send .initrd-tmp/fs/bin
# cp /bin/acx-license-send .initrd-tmp/fs/bin
```

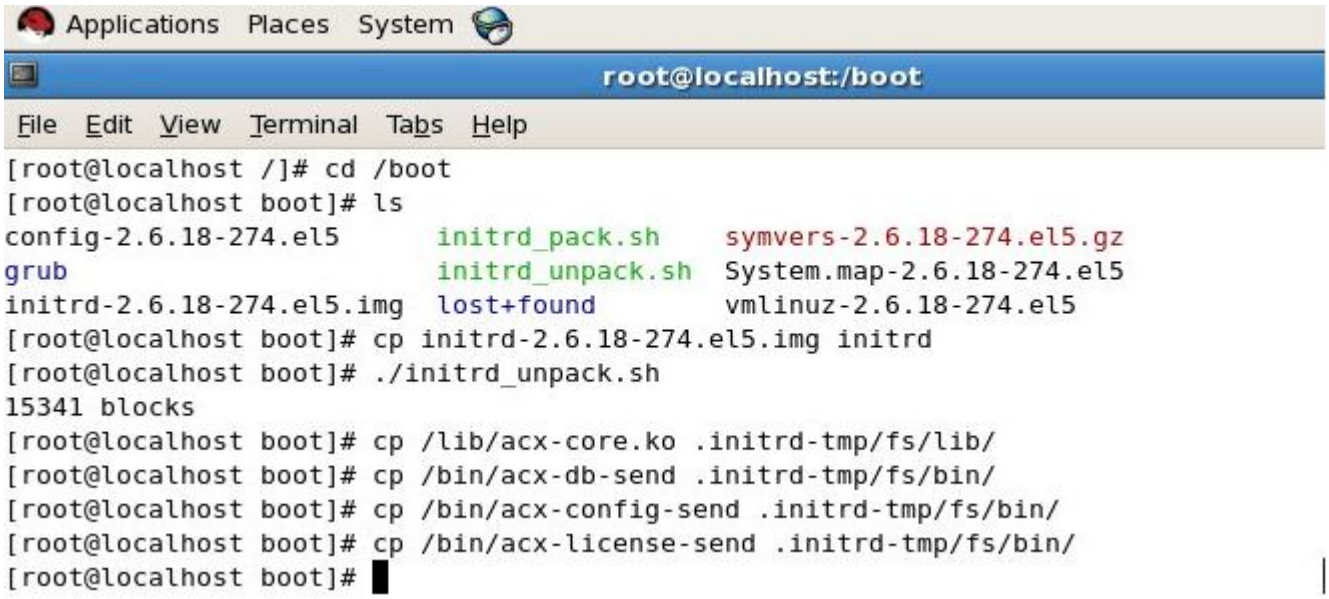

Рисунок 13 – Настройка образа начальной загрузки

г) непосредственно перед выполнением switchroot (перемонтированием корневой файловой системы из /sysroot[ro] в /[rw]) добавить в файл .initrd-tmp/fs/init следующее (рисунок 14):

```
#############################################################
echo "Starting AccordX security module"
/sbin/insmod /lib/acx-core.ko
echo "Loading AccordX license"
/bin/acx-license-send /sysroot/etc/accordx/license.accordx
echo "Loading AccordX config"
/bin/acx-config-send /sysroot/etc/accordx/acx-config.json
echo "Loading AccordX database"
/bin/acx-db-send /sysroot/etc/accordx/db.json
#############################################################
```

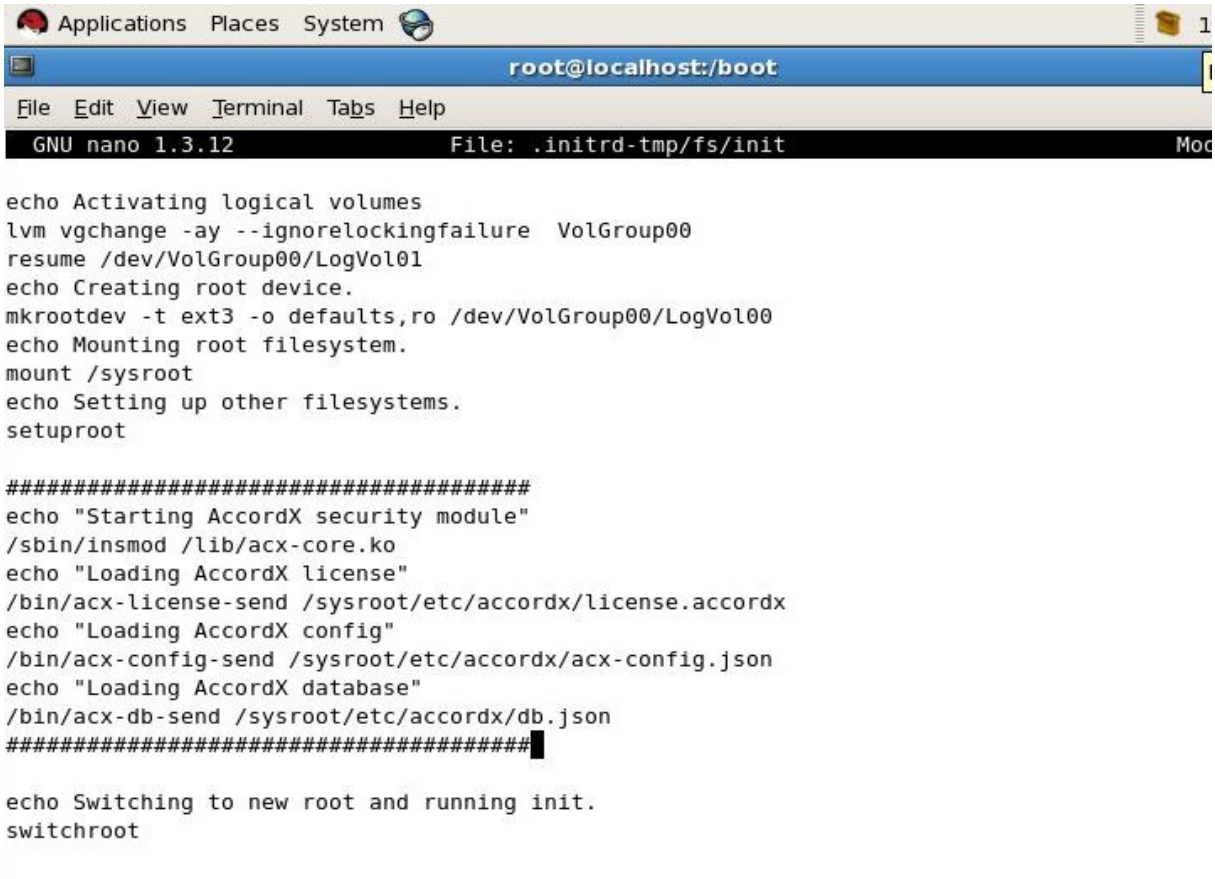

Рисунок 14 – Информация о загрузке монитора РД в скрипте init

Дополнительно необходимо убедиться в наличии в .initrd-tmp/fs/sbin бинарного файла insmod (иногда вместо insmod в initrd может присутствовать только modprobe – в данном случае можно скопировать insmod из целевой системы в соответствующую папку в initrd, а также убедиться в том, что зависимостей для выполнения insmod в initrd достаточно).

д) запаковать образ initrd с помощью скрипта из пакета *acx-core:*

```
# ./initrd_pack.sh
```

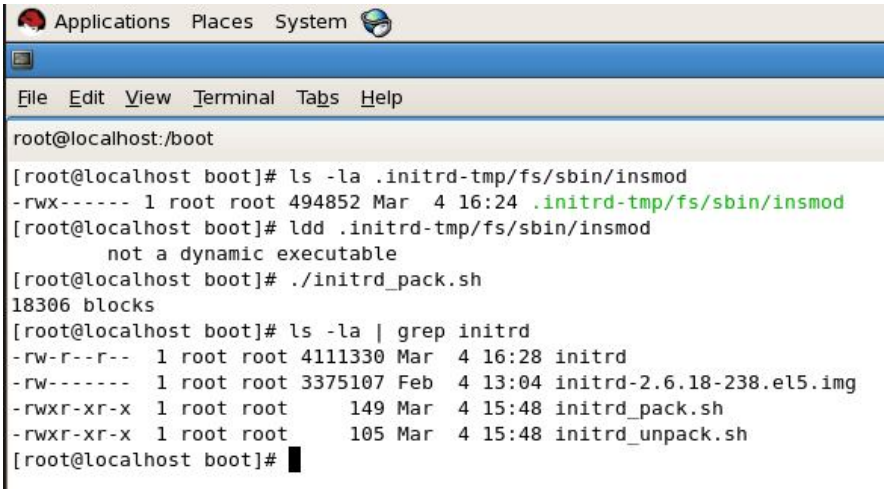

Рисунок 15 – Проверка наличия файла insmod, запаковка образа initrd

В итоге файл /boot/initrd будет содержать всё необходимое для корректной загрузки монитора разграничения доступа.

В Н И М А Н И Е !

При распаковке/запаковке initrd с помощью скриптов /boot/initrd_pack.sh и /boot/initrd_unpack.sh (которые по умолчанию распаковывают/запаковывают файл с именем /boot/initrd) необходимо учитывать, что в некоторых ОС Linux (например, SUSE Linux Enterprise Server и в многих других) в /boot уже существует символическая ссылка initrd, указывающая на оригинальный файл initramfs. В связи с этим, либо на время редактирования initrd нужно переименовать символическую ссылку initrd, либо изменить в скриптах initrd_pack/initrd_unpack соответствующее значение.

4.5.3 Настройка загрузки файла intird

Теперь для запуска ОС вместе с монитором разграничения доступа необходимо прописать полученный файл initrd для автовыбора в загрузчике (рассмотрен загрузчик grub) вместо [current initrd] (рисунок 16).

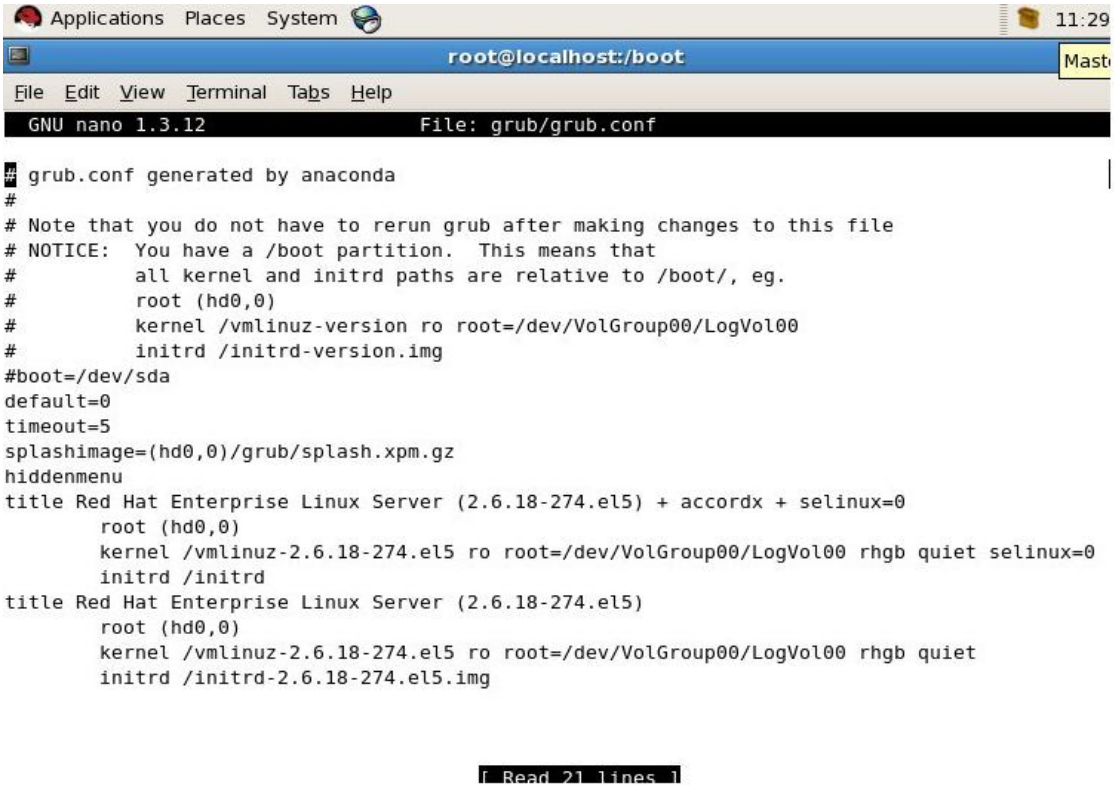

Рисунок 16 – Файл initrd прописан для автовыбора в загрузчике grub

В Н И М А Н И Е !

В приведенном примере показан конфигурационный файл загрузчика grub в момент настройки СПО «Аккорд-Х К». По окончании настройки (перед вводом СПО «Аккорд-Х К» в эксплуатацию) следует выполнить следующее:

1. исключить все таймауты в загрузчике (установить значения таймаутов в 0);

2. исключить возможность выбора альтернативных вариантов загрузки (на выбор должен быть доступен всего один вариант загрузки с запуском СПО «Аккорд-Х К»);

3. исключить возможность динамического изменения настроек загрузчика, в т.ч. возможных вариантов загрузки (в случае загрузчика grub для этого достаточно задать пароль – grub password);

4. в разделе boot не следует хранить лишних объектов (например, старые версии ядра Linux, старые версии initrd и т.п.);

5. для загрузчика следует оставить наименьшее количество возможных расширений/модулей (если нет необходимости использовать специфические файловые системы, то лучше удалить эти модули).

4.5.4 Контроль доступа к информации на внешних устройствах

Для корректного сопоставления пользователя с устройством (внешним носителем информации), а также для обеспечения возможности контроля ввода-вывода на такие устройства администратору безопасности необходимо провести ряд дополнительных настроек ОС.

Т.к. в ОС семейства Linux любой поддерживаемый внешний носитель информации можно подключить в любую точку монтирования (путь в файловой системе) при наличии достаточных прав, в ОС должен быть описан порядок монтирования тех или иных носителей информации в строго отведенные точки монтирования (например, их можно создать в каталоге /mnt). Для этого необходимо отредактировать файл /etc/fstab, в котором описываются записи с доступными точками монтирования. Формат записи /etc/fstab:

`fs mountpoint fstype mountopts fsreq fsck`

Где:

- **fs** – device (например, /dev/sdb), LABEL (например, boot) или UUID (например, 3e6be9de-8139-11d1-9106-a43f08d823a6) подключаемого устройства / раздела устроства. Также для идентификации нескольких разделов можно использовать PARTUUID и PARTLABEL (доступно для GPT-дисков)

  т.е. монтируемое устройство (раздел) можно определить как:

  /dev/sdb1 (неоднозначное определение)

  или

  LABEL=boot (неоднозначное определение)

  или

  UUID=3e6be9de-8139-11d1-9106-a43f08d823a6

  (однозначное определение для ФС, поддерживающихся в Linux)

- **mountpoint** – точка монтирования устройства (например, /mnt/diskA);
- **fstype** – тип файловой системы (adfs, affs, autofs, coda, coherent, cramfs, devpts, efs, ext2, ext3, hfs, hpfs, iso9660, jfs, minix, msdos, ncpfs, nfs, ntfs, proc, qnx4, reiserfs, romfs, smbfs, sysv, tmpfs, udf, ufs, umsdos, vfat, xenix, xfs и, возможно, другие). Список поддерживаемых текущим ядром ОС файловых систем можно просмотреть в файле /proc/filesystems
- **mountopts** – опции монтирования (см. mount(8) в man), в случае если в системе не поддерживается автомонтирование – существует опция user;
- **fsreq** – опция для выполнения резервирования (dump);
- **fsck** – опция для вызова fsck для проверки файловой системы.

Для определения UUID и LABEL для носителей информации можно воспользоваться утилитой blkid или lsblk (при подключении такого носителя информации в СВТ).

Администратор должен описать всевозможные подключаемые устройства (идентифицируя их, желательно, по UUID) и задать для каждого из них свою точку монтирования (например в каталоге /mnt/diskA, /mnt/diskB и т.п.). После чего для каждого пользователя можно задать права в рамках дискреционной политики доступа Аккорд-Х К на доступ к этим точкам монтирования, а для точек монтирования можно задать иерархические метки с уровнем конфиденциальности или добавить некоторые объекты в списки контроля целостности – всё зависит от решаемых задач по контролю за внешними носителями информации.

4.5.5 Активизация подсистемы разграничения доступа к ресурсам ПЭВМ

После выполнения описанной выше последовательности действий по установке и настройке СПО «Аккорд-Х К» необходимо выполнить активацию подсистемы разграничения доступа, скопировав файл лицензии license.accordx в каталог /etc/accordx/.

Если файла лицензии не будет найдено или он окажется неверным, будет вызвана паника ядра (kernel panic) с соответствующей информацией об этом («file not found» или «acx-core: invalid license!») и загрузка ОС не продолжится.

После того, как файл лицензии будет помещен в корневой каталог, следует выполнить перезагрузку компьютера, после которой производится загрузка нового файла initrd, сформированного в процессе выполнения пп. 4.5.2-4.5.3, и подсистема разграничения доступа к ресурсам ПЭВМ активизируется.

4.5.6 Перезагрузка ОС в мягком режиме работы СПО «Аккорд-Х К»

На последней стадии установки и настройки СПО «Аккорд-Х К» необходимо произвести перезагрузку ОС с установленным «мягким» режимом работы СПО «Аккорд-Х К» (устанавливается с помощью команды «*acx-admin config set enable-soft-mode true»;* при автосоздании файла конфигурации «мягкий» режим установлен по умолчанию).

В данном режиме пользователи смогут выполнить операцию login по заданным на этапе настройки данным для идентификации, но политики разграничения доступа для них будут неактивны (т.е. будет работать только разграничение доступа самой ОС Linux). В мягком режиме необходимо совершить как можно больше действий, симулирующих работу пользователя (в основном здесь учитывается запуск каких-либо сервисов/процессов, а не работа с данными/программами и т.п.).

После этого необходимо из журнала работы СПО «Аккорд-Х К» в «мягком» режиме дополнить БД пользователей необходимыми субъектами доступа

(shadow – т.е. пользователями, которые не осуществляют прямой операции login, но от имени которых могут запускаться определенные процессы в ОС, например, gdm-session-worker или apache и т.д.), выполнив команду «*acx-admin log makeshadows /var/log/accordx/****», где *** - имя файла журнала работы «Аккорд-Х К» в «мягком» режиме.

Просмотреть пользователей shadow можно с помощью команды «*acx-admin db show –vv*».

После корректного создания пользователей типа shadow нужно включить ту или иную политику разграничения доступа (т.е. выключить «мягкий» режим) и перезагрузиться.

4.5.7 Некоторые особенности настройки СПО «Аккорд-Х К»

В процессе настройки СПО «Аккорд-Х К» администратору БИ необходимо учитывать следующие особенности:

а) В зависимости от логики работы контроля целостности может потребоваться НЕ передавать в качестве параметров ядру опции splash/quite/rhgb(RHEL), т.к. запрос дальнейшего действия (как в примере для static_icl в скриптах инициализации) при их наличии может не отображаться в момент загрузки.

б) Для корректной работы некоторых компонентов «Аккорд-Х К» (PAM, модули по работе с данными для идентификации) при работающем SELinux необходимо:

- либо отключить SELinux:
- *–– передав при загрузке в параметре ядра selinux=0 (см, например, рисунок 16) или*
- –– записав в /etc/selinux/config SELINUX=permissive (однако данный метод может не сработать и PAM-модули в СПО «Аккорд-Х К» будут заблокированы SELinux);
- либо добавить наш PAM в SELinux (данный метод также может не работать до конца); пример:

```
* semanage fcontext -a -t textrel_shlib_t
'/lib/security/pam_acx_marsh.so'
restorecon -v '/lib/security/pam_acx_marsh.so'

* semanage fcontext -a -t SIMILAR_TYPE 'tmusb0'
restorecon -v 'tmusb0'
```

в) После активации подсистемы разграничения доступа и перезагрузки ОС в случае внесения каких-либо изменений в файл конфигурации или БД пользователей Аккорд-Х К (например, с помощью утилит acx-admin*, под изменениями понимаются любые изменения этих файлов - редактирование паролей пользователей, добавление/удаление пользователей и т.п.) для учета таких изменений необходимо выполнить перезагрузку ОС. Без перезагрузки в СПО «Аккорд-Х К» будут активны БД и файл конфигурации, которые были актуальны на момент последней загрузки ОС.

4.6 Установка и настройка подсистемы контроля печати «Аккорд-X K»

Подсистема контроля печати СПО «Аккорд-X K» представляет собой модуль (фильтр) штатной подсистемы печати Linux CUPS. Модуль представляет собой модификацию фильтра pstops, который отрабатывает фактически последним в цепочке модулей CUPS для формирования документа, готового к отправке на печать на тот или иной принтер, и обеспечивает выполнение следующих функций:

- возможность принудительной печати углового, нижнего, итогового штампов на печатаемом документе;
- настройка вида штампов в печатаемом документе;
- отказ от печати штампов на документе;
- проверку прав печати на заданном принтере;
- протоколирование всех инициированных задач печати в журнале подсистемы печати.

Модуль контроля печати Аккорд-X K предназначен для перехвата потока данных, проходящих через фильтры штатной подсистемы печати CUPS, их обработки и внесения изменений, согласно данным, полученным от монитора разграничения доступа Аккорд-X K (имя субъекта, уровень доступа), настройкам, указанным в файлах конфигурации, и настройкам, заданным вручную пользователем (запрашиваются отдельно в диалоговом окне), имеющим на это полномочия.

В зависимости от настроек модуль позволяет маркировать каждую страницу выводимого на печать документа следующими реквизитами:

- ФИО пользователя;
- Дата и время печати документа;
- Учетный номер документа;
- Номер страницы и общее число страниц текущего документа;
- Логическое имя принтера;
- Номер экземпляра документа;
- Адрес отправления;
- Телефон исполнителя;
- Уровень конфиденциальности документа;
- Название документа и используемой программы (если оно передано);
- Имя компьютера;
- Наименование АС

Дополнительно пользователю, выводящему на печать документы, можно разрешить изменять следующий набор данных:

- Название документа;

- Гриф секретности (см. особенности ниже);
- ФИО пользователя;
- Учетный номер документа;
- Телефона исполнителя;
- Адреса отправки.

Гриф секретности документа может быть указан пользователем только с учетом следующего правила - гриф секретности документа не должен превышать уровня доступа пользователя. По умолчанию опция с возможностью изменять гриф секретности у пользователей не установлена (уровень секретности передается от монитора разграничения доступа).

В подсистеме контроля печати СПО «Аккорд-X K» реализована возможность журналирования процедуры печати (журнал ведется отдельно от событий подсистемы разграничения доступа в /usr/lib/cups/filter). Данные, записываемые в Журнал, аналогичны данным, выводимым в штампы. Дополнительно в журнал записывается статус выполнения задачи.

При настройке подсистемы печати Аккорд-X K необходимо иметь ввиду, что штатная подсистема печати Linux будет заменена. Однако в случае некорректной работы всегда можно переустановить подсистему печати из официального репозитория (отдельный пакет cups).

4.6.1 Установка модуля контроля печати

Модуль контроля печати поставляется в пакете acx-print. Для установки модуля необходимы следующие зависимости - cups-devel, cups-libs (в зависимости от дистрибутива названия могут отличаться). Перед установкой модуля необходимо убедиться в корректной работе подсистемы контроля доступа Аккорд-X K и монитора разграничения доступа.

До установки модуля контроля печати необходимо загрузить с официального сайта CUPS (http://cups.org) пакет cups-1.4.2.tar.gz, распаковать и установить его, например из консоли:

```
$ tar xzvf cups-1.4.2.tar.gz
$ cd cups-1.4.2
$ ./configure
$ make
$ su (получение прав суперпользователя для дальнейшей установки пакета)
# make install
```

После установки CUPS необходимо корректным образом настроить доступные принтеры (подробнее см. официальную документацию CUPS). Только после печати пробной страницы необходимо переходить к установке подсистемы контроля печати Аккорд-X K (таким образом убедившись, что печать вообще возможна).

После установки cups версии 1.4.2, необходимо установить пакет acx-print-***.rpm (вместо *** указать текущую версию пакета acx-print из

дистрибутива Аккорд-X K), игнорируя зависимости и предупреждения (опция --force):

```
# rpm -ihv acx-print-1.0.1.i686.tar.gz --force --nodeps
```

Далее нужно убедиться, что в вашем дистрибутиве установлена утилита zenity:

```
$ zenity --help
```

Если после ввода команды выше появилась справка, пакет zenity уже установлен в системе. Если справки не появилось - установите пакет zenity любым подходящим для вас образом (через пакетный менеджер, загрузив и установив пакет самостоятельно, либо собрав и установив из исходных кодов).

4.6.2 Необходимые настройки ОС

Для корректного функционирования модуля контроля печати СПО «Аккорд-X K» необходимо внести некоторые изменения в ОС:

1. в /etc/passwd псевдо-пользователю lp установить шел /bin/bash, таким образом строка должна иметь следующий вид:

```
lp:x:4:7:lp:/var/spool/lpd:/bin/bash
```

2. Выключить SELinux (этот шаг может потребоваться выше для корректной работы PAM-модулей Аккорд-X K).

3. Выполнить следующие команды от имени пользователя root:

```
# cd /var/spool/lpd
# mkxauth -u lp -c
```

4. При каждом старте системы необходимо выполнять:

```
# cd /var/spool/lpd
# xhost +
```

Данные команды можно прописать в соответствующие скрипты загрузки ОС в зависимости от конкретного дистрибутива.

4.6.3 Настройка параметров модуля контроля печати

После установки пакета acx-print в /usr/lib/cups/filter/accord.users записывается стандартный файл-шаблон с настройками для конкретного пользователя (см. подробнее Приложение 5). Для всех пользователей, которым планируется разрешить маркированную печать, в /usr/lib/cups/filter/accord.users/[username].cnf необходимо прописать список доступных принтеров:

```
printer=HP\ Color\ LaserJet\ 3800,1,2
```

Имя принтера в [username].cnf должно совпадать с названием файла в /etc/cups/ppd/printername.ppd без учета расширения (т.е. для названия файла printername.ppd необходимо прописать printer=printername). Также необходимо учитывать пробельные и прочие символы и вводить их после символа "\"

Общие настройки печати приведены в файле /usr/lib/cups/filter/accord.cnf (см. Приложение 6).

Для проверки работы модуля контроля печати нужно попробовать вывести на печать некоторый файл, выполнив следующую команду "lpr FILENAME -P HP\ Color\ LaserJet\ 3800", где FILENAME - полный путь до печатаемого файла, HP\ Color\ LaserJet\ 3800 - название принтера, на котором разрешена печать в конфигурационном файле. Обращаем внимание на то, что для корректной работы модуля контроля печати остальные компоненты Аккорд-X K должны быть настроены и запущены (т.е. должны быть проделаны все действия из раздела 4.4)

5 ЭКСПЛУАТАЦИЯ СПО «АККОРД-Х К»

5.1.1 Основные задачи, решаемые администратором БИ при эксплуатации СПО «Аккорд-Х К»

При эксплуатации СПО «Аккорд-Х К» администратор БИ решает следующие задачи:

- поддерживает средства защиты СПО «Аккорд-Х К» в работоспособном состоянии и контролирует правильность их работы;
- производит изменения в настройке средств защиты СПО «Аккорд-Х К» 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 над работой пользователей СВТ с внедренными средствами защиты СПО «Аккорд-Х К»;
- анализирует содержимое журнала регистрации событий, формируемого средствами СПО «Аккорд-Х К», и на этой основе вырабатывает предложения по совершенствованию защитных механизмов, реализуемых средствами СПО «Аккорд-Х К», принимает необходимые меры по совершенствованию системы защиты информации в целом.

В Н И М А Н И Е !

Непрерывная организационная поддержка функционирования средств защиты СПО «Аккорд-Х К» предполагает обеспечение строгого соблюдения всеми пользователями требований СБИ (администратора БИ).

5.1.2 Вход в ОС в рамках действия СПО «Аккорд-Х К»

При загрузке СВТ, защищенного СПО «Аккорд-Х К», на начальном этапе загрузки ОС загружается СПО «Аккорд-Х К» (из образа начальной загрузки initrd). При этом на экран выводится информация об успешном выполнении загрузки монитора разграничения доступа «Аккорд-Х К», его конфигурации и БД (рисунок 17) (в случае какой-либо ошибки вызывается паника ядра с указанием причины – превышен таймер ожидания БД, неправильная лицензия и т.п. – и дальнейшая загрузка ОС не осуществляется). Сразу после этого активируются и вступают в действие механизмы защиты, которые включены в данных о конфигурации МРД (их можно изменить в ходе работы ОС с использованием утилиты acx-admin config и утилиты загрузки данных конфигурации в МРД acx-config-send).

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

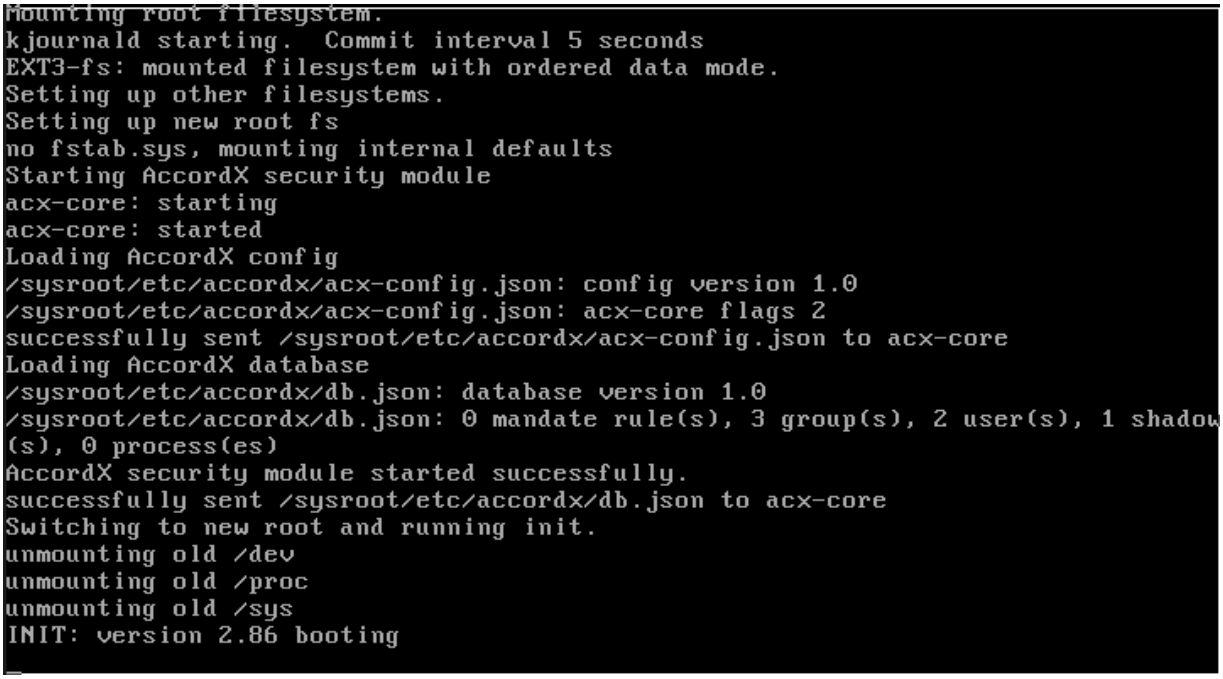

Рисунок 17 – Загрузка модуля разграничения доступа «Аккорд-X K»

Необходимо отметить, что информацию на рисунке выше можно легко пропустить, т.к. (в зависимости от СВТ) процесс начальной загрузки может осуществляться очень быстро.

Далее на последнем этапе загрузки ОС вместо штатной процедуры идентификации и аутентификации в ОС PAM-модуль «Аккорд-X K» предложит предъявить данные для идентификации (рисунок 18). Необходимо ввести данные для идентификации или предъявить соответствующий идентификатор пользователя (рисунок 19).

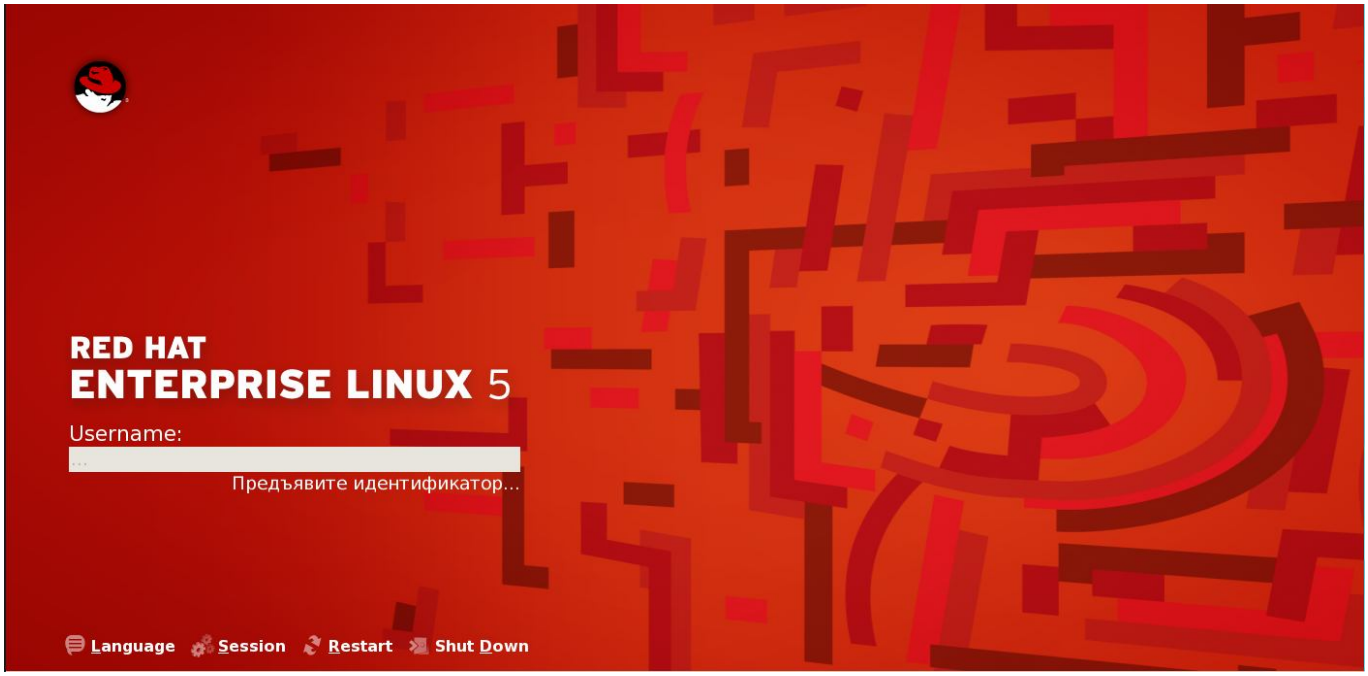

Рисунок 18 – Запрос данных для идентификации

После предъявления данных для идентификации в появившемся поле «Введите пароль» следует ввести соответствующий пароль пользователя, установленный для него в «Аккорд-X K» (рисунок 19).

Рисунок 19 – Запрос пароля

После выполнения процедуры идентификации/аутентификации пользователя и входа в ОС начинают работать ПРД, которые были заданы ему на этапе настройки.

В Н И М А Н И Е !

Работа в ОС Linux с установленным СПО «Аккорд-Х К» отличается (от работы в ОС без СПО «Аккорд-Х К») только другой процедурой идентификации/аутентификации и возможными запретами на получение доступа к какому-либо объекту или файлу.

5.1.3 Примеры выполнения установленных ПРД

Рассмотрим некоторые примеры выполнения установленных политик разграничения доступа (которые были оптимистично заданы в разделе с установкой и настройкой).

Пример 1. Демонстрация работы динамического контроля целостности, не позволяющего запускать на выполнение файлы, целостность которых нарушена (контроль целостности осуществляется непосредственно при запуске на выполнение):

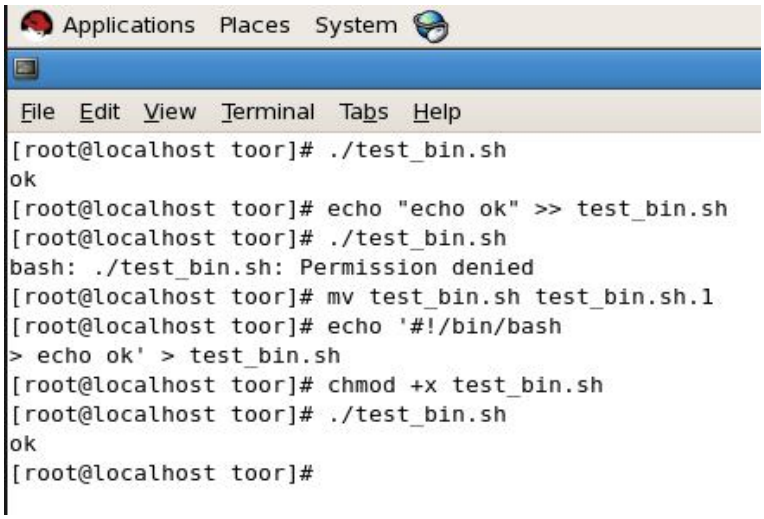

Рисунок 20 – Запрет запуска на выполнение файлов, целостность которых нарушена

Пример 2.Демонстрация работы ПРД, когда пользователю запрещено переходить в каталог (при работе в консольном режиме):

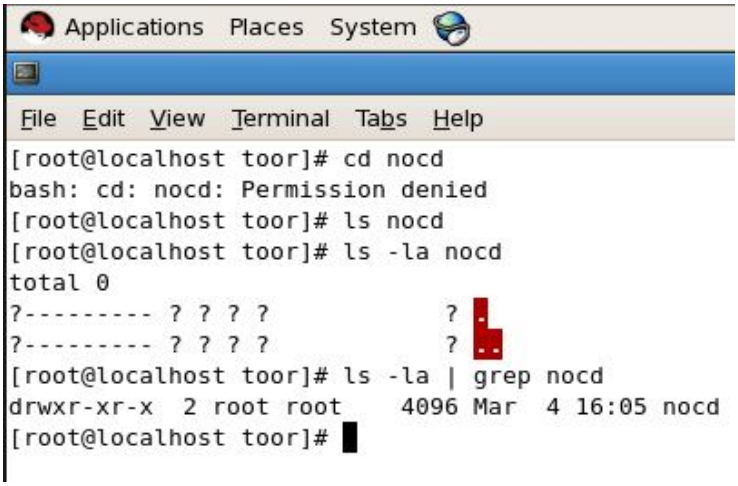

Рисунок 21 – Запрет перехода в каталог (при работе в консольном режиме)

При работе с использованием GUI это выглядит следующим образом:

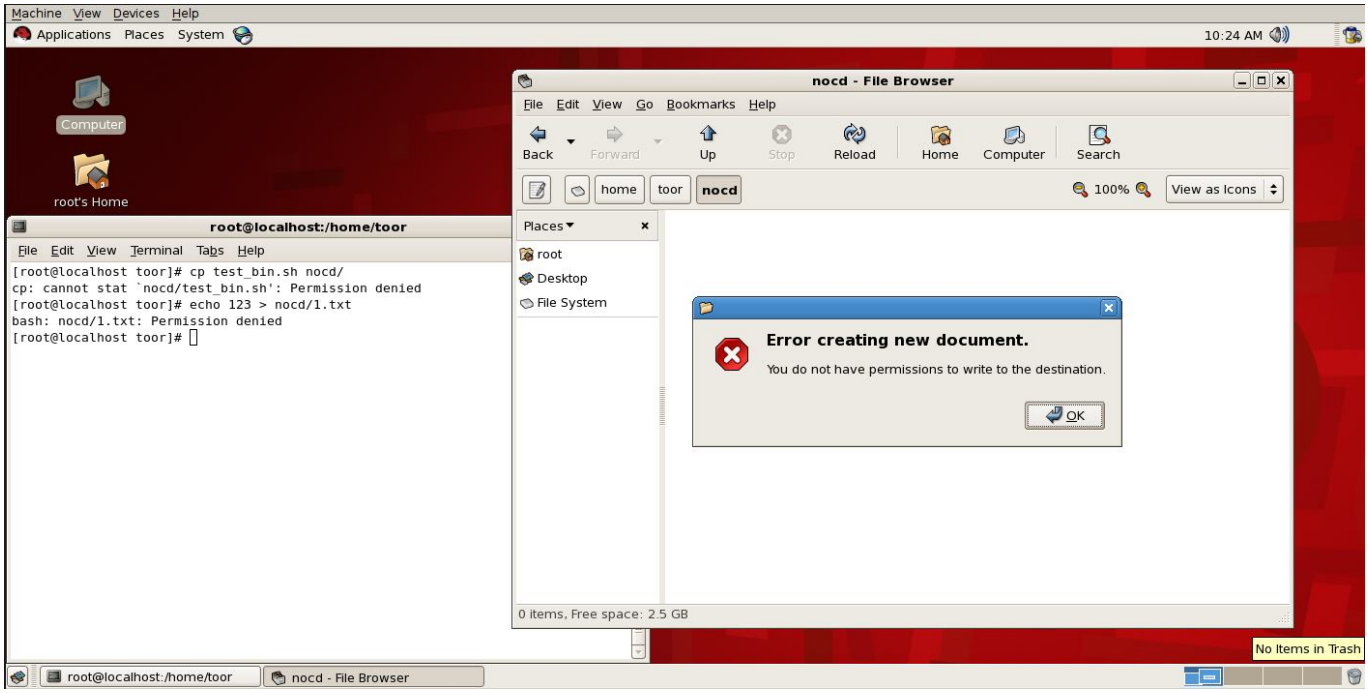

Рисунок 22 – Запрет перехода в каталог (при работе с использованием GUI)

Пример 3. Демонстрация работы ПРД, когда пользователю запрещено запускать на выполнение программы:

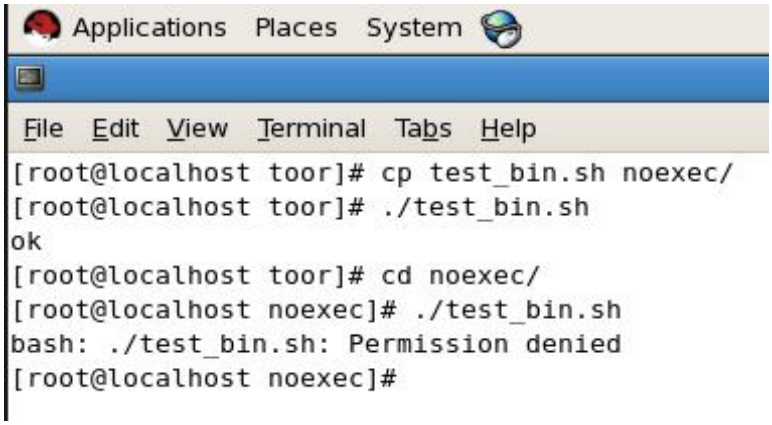

Рисунок 23 – Запрет запуска на выполнение программ

Пример 4. Демонстрация работы ПРД, когда пользователю запрещено открывать на чтение файлы (при работе в консольном режиме):

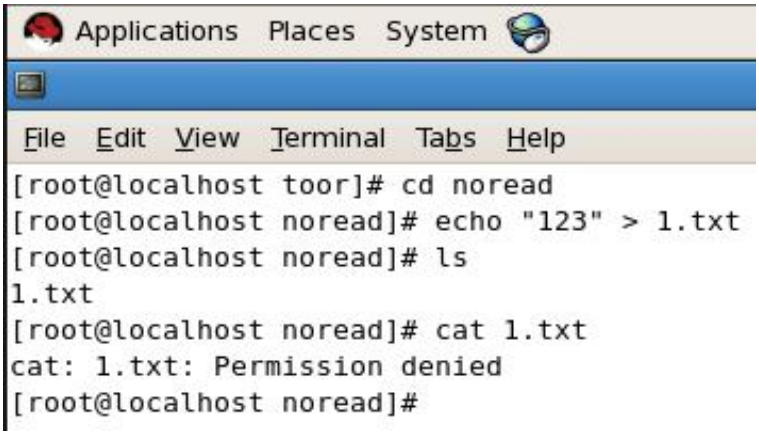

Рисунок 24 – Запрет открытия файлов на чтение (при работе в консольном режиме)

При работе с использованием GUI это выглядит следующим образом:

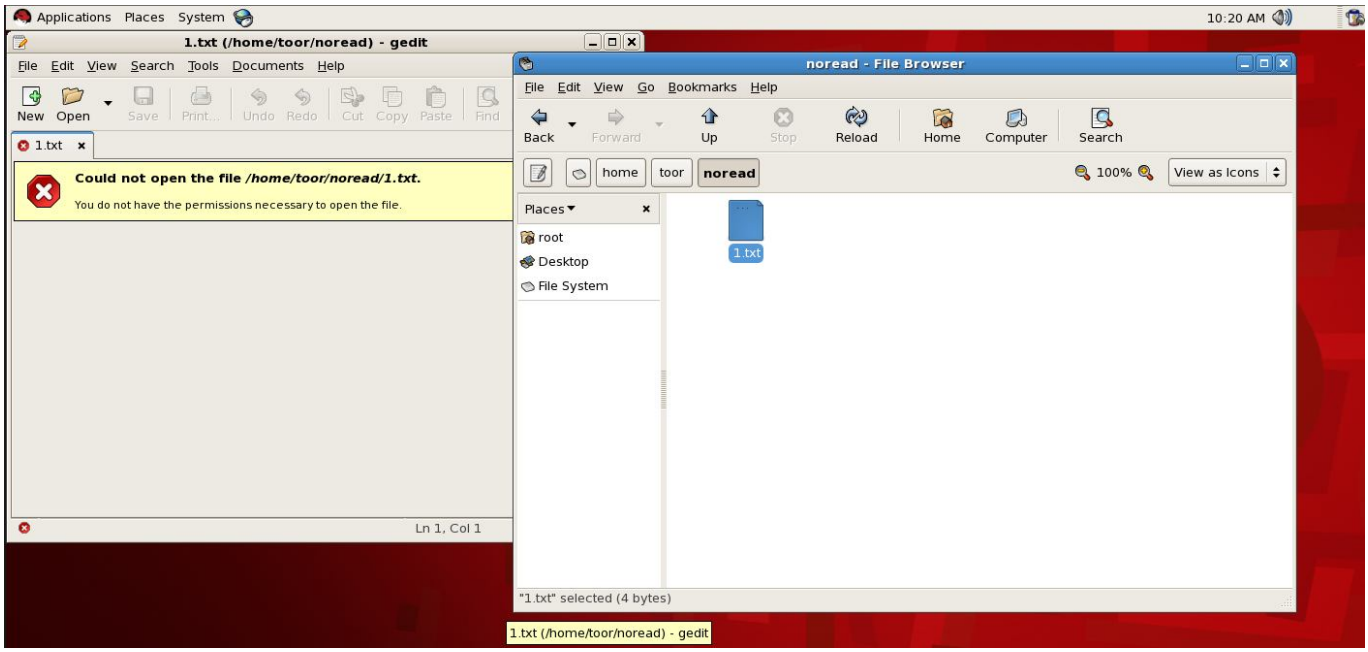

Рисунок 25 – Запрет открытия файлов на чтение (при работе с использованием GUI)

Пример 5. Демонстрация работы ПРД, когда пользователю запрещено записывать данные в объекты (обратите внимание: не создавать объекты на запись, а именно выполнять операции записи данных в объекты).

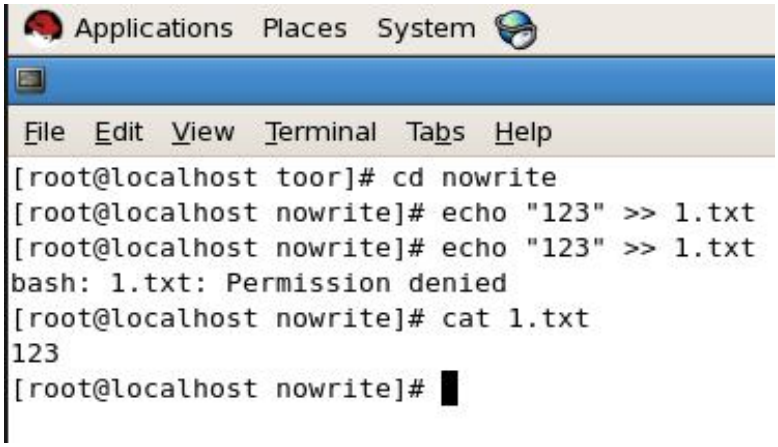

Рисунок 26 – Запрет на запись данных в объект (при работе в консольном режиме)

При работе с использованием GUI это выглядит следующим образом (документ имеет статус «read-only», кнопка <Сохранить> недоступна):

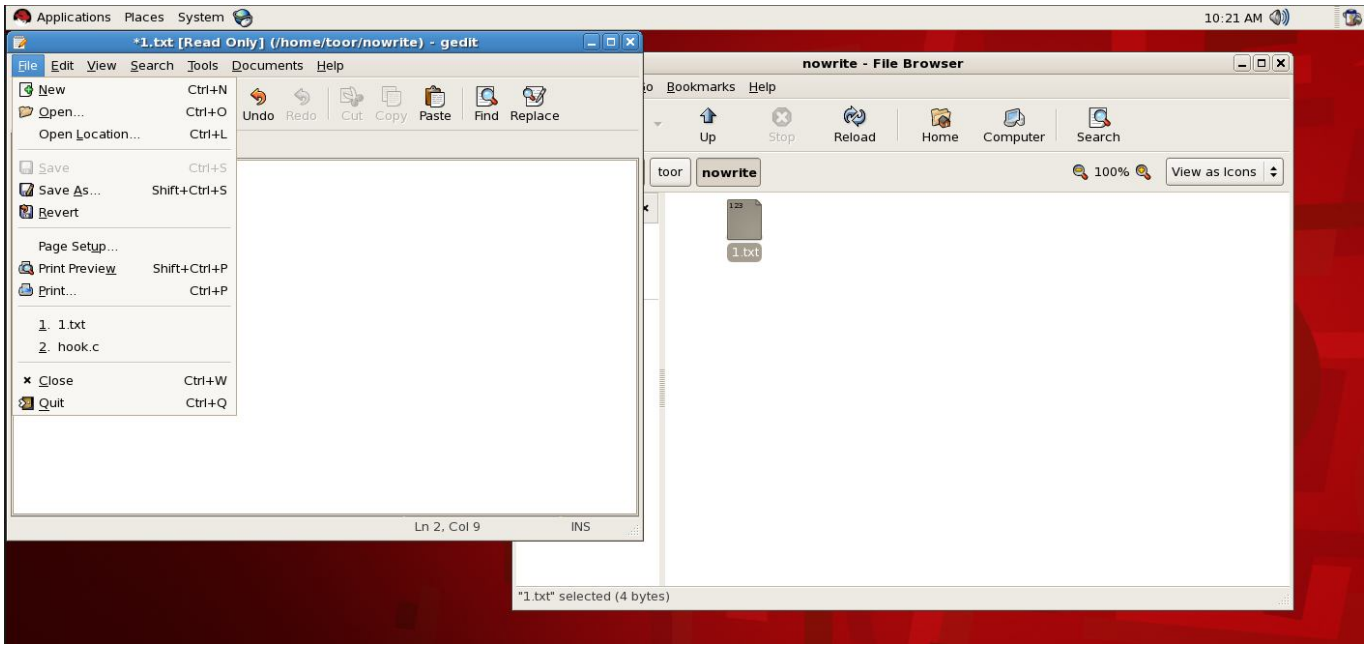

Рисунок 27 - Запрет на запись данных в объект (при работе с использованием GUI)

5.1.4 Работа с журналом регистрации событий

Как для каталогов, так и для отдельных файлов, в «Аккорд-X K» присутствует возможность установки опции регистрации в регистрационном журнале доступа к каталогу и его содержимому. Регистрация осуществляется следующим образом:

- 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;
- 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.

Утилита администрирования СПО «Аккорд-X K» acx-admin log предоставляет возможность просмотра, вывода на печать и архивации журнала регистрации событий СПО «Аккорд-X K».

Администратор БИ может просматривать журнал регистрации событий в «Аккорд-X K» (/var/log/accordx***, рисунок 28) с помощью вызова вида `acx-admin-log show -m -C /var/log/accordx....`

Например:

`acx-admin-log show -m –C /var/log/accordx/shadow_root_20140401_10:00`,

где

shadow – тип субъекта доступа (от имени которого создается журнал);

root – имя субъекта доступа;

20140401 – дата создания журнала;

10:00 – время создания журнала в UTC.

```
091     10:11:33[1397124693.825]        2426    2456    err     subj    setuid  user    user
root    root 0  root 0
092     10:11:43[1397124703.420]        2426    2456    err     subj    setuid  user    user
root    root 0  root 0
093     10:11:48[1397124708.006]        2947    2974    max     fs      open    int     user
root    /bin/bash       /test/1.sh
094     10:11:48[1397124708.006]        2947    2974    max     fs      open    int     user
root    /bin/bash       /test/1.sh
095     10:11:49[1397124709.657]        2944    2947    max     fs      chdir   discr   user
root    /bin/bash       /test/nocd/
096     10:11:49[1397124709.657]        2944    2947    max     fs      chdir   discr   user
root    /bin/bash       /test/nocd/
097     10:11:51[1397124711.257]        2947    2975    max     fs      chdir   discr   user
root    /bin/ls /test/nocd/
098     10:11:51[1397124711.257]        2947    2975    max     fs      chdir   discr   user
root    /bin/ls /test/nocd/
099     10:11:51[1397124711.257]        2947    2975    max     fs      chdir   discr   user
root    /bin/ls /test/nocd/
100     10:11:54[1397124714.704]        2947    2976    max     fs      chdir   discr   user
root    /bin/ls /test/noroot/
101     10:11:54[1397124714.704]        2947    2976    max     fs      chdir   discr   user
```

Рисунок 28 – Просмотр журнала регистрации событий

В журнале фиксируются все события доступа субъектов доступа к объектам доступа (начиная с самого раннего этапа загрузки Linux). Журнал отображается в виде таблицы. Каждая строка таблицы соответствует одному событию, зарегистрированному в журнале.

Записям в журнале соответствует время в формате HH:MM:SS[time] (где HH:MM:SS – время регистрации события в UTC, time – время, отсчитываемое с момента загрузки ядра ОС), например 10:00:01[1390936318.188].

Для удобства просмотра и анализа информации присутствует возможность фильтрации по одному или нескольким полям таблицы (см. подраздел «Работа с модулем acx-admin log» Приложения 2).

Подробное описание содержимого журнала регистрации см. в Приложении 3.

6 СНЯТИЕ СРЕДСТВ ЗАЩИТЫ СПО «АККОРД-X К»

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

В Н И М А Н И Е !

Снятие (отключение) средств защиты СПО «Аккорд-X К» разрешено только администратору БИ (супервизору).

Для снятия защиты Администратору БИ необходимо отключить подсистему разграничения доступа (перейти на использование штатного initrd ОС или отключить механизмы разграничения доступа с помощью acx-admin config/acx-config-send).

7 ПРАВОВЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ СПО «АККОРД-Х К»

Специальное программное обеспечение «Аккорд-Х К» v.1.0 и сопутствующая документация защищены законом России об авторских правах, а также положениями Международного Договора. Любое использование СПО «Аккорд-Х К» в нарушение закона об авторских правах или в нарушение положений ЭД на СПО «Аккорд-Х К» 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 СПО «Аккорд-Х К» для использования потребителем, приобретшим СПО АККОРД™ в установленном порядке. Ни при каких обстоятельствах программное обеспечение «Аккорд-Х К» не распространяется между другими предприятиями (фирмами) и лицами.

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

При покупке и применении СПО «Аккорд-Х К» предполагается, что Вы знакомы с данными требованиями авторов разработки и изготовления СПО «Аккорд-Х К»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 СПО АККОРД. ОКБ САПР использует для поддержки связи с пользователями адрес SUPPORT@OKBSAPR.RU. Нам удобнее принимать и обрабатывать Ваши сообщения именно таким образом.

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 СПО «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 СПО АККОРД™:

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

2. Устанавливать СПО «Аккорд-Х К» в СВТ и организовывать ее эксплуатацию с внедренными средствами защиты.

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.

В Н И М А Н И Е !

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 СПО «Аккорд-Х К» и оказывать помощь в части организации работы на СВТ с внедренным СПО «Аккорд-Х К».

5. Контролировать на целостность файлы СПО разграничения доступа.

6. Выявлять возможные каналы НСД к информации при применении СПО «Аккорд-Х К», готовить предложения по их устранению.

7. Систематически анализировать состояние СПО «Аккорд-Х К» и его отдельных средств, периодически проводить их тестирование и проверку защитных функций СПО «Аккорд-Х К», о чем делать отметку в формуляре.

8. Регулярно анализировать содержание системного журнала и разрабатывать меры по исключению неправильного применения СПО «Аккорд-Х К» пользователями.

В Н И М А Н И Е !

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 (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, СПО «Аккорд-Х К» 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. Описание утилит администрирования acx-admin

Общие сведения

Утилиты из состава acx-admin* предназначены для работы с базой данных пользователей и настройками, загружаемыми в МРД.

БД данных до загрузки в МРД представляет собой файл с данными формата JSON, описывающий все субъекты и объекты доступа, а также правила разграничения доступа и списки контроля целостности (статический и динамический контроль целостности).

С помощью acx-admin можно работать со следующими сущностями (соответствуют параметрам командной строки OBJECT):

1) config - файлом конфигурации, в котором указывается путь до файла с БД и т.д.

2) db - файлом БД (вывести все записи, загрузить БД в МРД, синхронизировать с другими БД ОС, очистить БД и т.д.)

3) group - группами пользователей/shadow/процессов (создание, удаление, редактирование настроек групп)

4) user - пользователями БД (создание, удаление, редактирование пользователей в БД, создание правил разграничения доступа к объектам, задание уровня доступа в рамках разграничения доступа на основе иерархических меток, создание списков контроля целостности, настройка разрешенных часов работы пользователя и т.п.)

5) shadow - shadow БД (создание, удаление, редактирование субъектов типа shadow)

6) process - процессами БД (создание, удаление, редактирование субъектов/объектов типа process)

7) acl - списками контроля доступа (формат 'объект ~ права доступа к объекту' для каждого субъекта/объекта, либо уровень конфиденциальности в рамках разграничения доступа на основе иерархических меток)

8) icl - списками контроля целостности (формат 'объект ~ контрольная сумма')

9) log – журналами МРД (нарушение целостности файлов, поставленных на контроль, попытки нарушения прав доступа и т.п.)

Для получения справки по работе с той или иной сущностью необходимо выполнить команду '#./acx-admin OBJECT --help', где в качестве OBJECT использовать одну из описанных сущностей.

Для каждой утилиты существует расширенная справка, вызываемая командой --help (например, #./acx-admin user add –help).

Подробнее о работе с каждой сущностью см. в соответствующих подразделах данного Приложения.

acx-admin config

Утилита acx-admin config предназначен для задания базовых настроек acx-admin и МРД, в частности, для задания пути до файла, содержащего базу данных пользователей.

acx-admin db

acx-admin db - утилита для работы с базой данных пользователей. Основные команды и опции данной утилиты описаны в таблице 1.

Таблица 1 – Основные команды и опции acx admin db

Команда	Опции/параметры команды	Комментарий
show		Вывести на экран информацию из БД (путь до файла БД указывается с помощью acx-admin config)
	#acx-admin db show	выводит краткую информацию (версия БД, количество групп, пользователей, shadow, process в БД).
	--verbose или -v	позволяет увеличивать детализацию вывода, например:
	#acx-admin db show -v	выведет дополнительно информацию по всем группам с указанием типа группы и количества сущностей в каждой группе, а также по глобальным спискам статического и динамического контроля целостности
	#acx-admin db show -v -v	выведет дополнительно краткую информацию по каждой сущности в каждой группе, а также сами списки статического и динамического контроля целостности. Для групп пользователей степень детализации 4 (т.е. опцию --verbose, -v необходимо написать 4 раза)+...+
	--mach, -m	позволяет вывести информацию в удобном для выделения нужных значений (удобном для парсинга) виде (для отделения значений друг от друга используются символы табуляции \t и переноса строк \n).
	-f <filename>	позволяет задать файл БД, отличный от файла БД в конфигурации acx-admin
send		Загрузить БД в acx-core (для данного действия потребуется пройти процедуру идентификации/аутентификации Администратора accordx)
	--verbose, -v или --quiet, -q	позволяют либо детализировать сообщения, выдаваемые при работе утилиты, либо скрыть их
	-f <filename>	позволяет задать файл БД, отличный от файла БД в конфигурации acx-admin
sync		Синхронизировать БД acx-db с другой БД
	--verbose, -v или --quiet, -q	позволяют либо детализировать сообщения, выдаваемые при работе утилиты, либо скрыть их
	--os, -o и -amdz, -a	с помощью данных опций выбирается БД-приемник, с которой будет осуществляться синхронизация (под синхронизацией в данном случае понимается добавление

Команда	Опции/параметры команды	Комментарий
		или изменение данных в БД-приемнике, которых либо нет, либо какие-то значения в этой БД отличаются от значений в acx-db т.е. acx-db является приоритетной базой данных и сама не изменяется)
	-f <filename>	позволяет задать файл БД, отличный от файла БД в конфигурации acx-admin
clear		Очистить БД acx-db
	--verbose, -v или --quiet, -q	позволяют либо детализировать сообщения, выдаваемые при работе утилиты, либо скрыть их
	-f <filename>	позволяет задать файл БД, отличный от файла БД в конфигурации acx-admin
verify		Проверить содержимое БД acx-db
	--verbose, -v или --quiet, -q	позволяют либо детализировать сообщения, выдаваемые при работе утилиты, либо скрыть их
	-f <filename>	позволяет задать файл БД, отличный от файла БД в конфигурации acx-admin

acx-admin group

acx-admin group - утилита для создания/удаления групп в БД. Основные команды и опции данной утилиты описаны в таблице 2.

Таблица 2 - Основные команды и опции acx admin group

Команда	Опции/параметры команды	Комментарий
acx-admin group add GROUPNAME		Создать группу соответствующего типа (user, shadow, process) в БД accordx
	-t [user|shadow|process]	задать тип группы (группа пользователей, shadow, process)
	-f [path]	определить путь к БД accordx вместо указанного в конфиге
acx-admin group delete GROUPNAME		Удалить группу из БД accordx (включая все учетные записи, существующие в группе)
	-f [path]	определить путь к БД accordx вместо указанного в конфиге
acx-admin group show GROUPNAME		Просмотреть информацию о группе с нужной степенью детализации выводимых атрибутов
	--verbose, -v	позволяют детализировать сообщения, выдаваемые при работе утилиты (например, раскрыть acl, icl или пользователей группы)
	--mach, -m	позволяют формировать вывод в машиночитабельном формате (с использованием табуляции, без пробелов)
	-f <filename>	позволяет задать файл БД, отличный от файла БД в конфигурации acx-admin
acx-admin group	-h, --help (например, #./acx-admin group --help)	Опция для просмотра подробной справки

acx-admin user

acx-admin user - набор утилит для редактирования пользовательских учетных записей Аккорд-X K и ОС. Основные команды и опции данного модуля описаны в таблице 3.

Таблица 3 - Основные команды и опции acx admin user

Команда	Опции/параметры команды	Комментарий
acx-admin user add USERNAME		Создать пользователя с заданными параметрами в БД accordx и в БД ОС (для создания в БД ОС требуются права суперпользователя ОС)
	-p PASSWORD	задать пароль нового пользователя (обязательный параметр)
	-t 'XX XXXXXXXXXXXX XX'	задать данные для идентификации (обязательный параметр)
	-u UID	задать UID пользователя (может задаваться автоматически очередной). Если пользователь автоматически создается в ОС - UID должен быть уникальный
	-b	задать флаг блокировки пользователя в accordx
	-w 'mon:XX:XX-XX:XX,XX:XX-XX:XX[;tue...]'	задать разрешенные часы работы пользователя (обязательный параметр) - можно задать пустое значение ''
	-a GROUPNAME	определить группу accordx, в которой необходимо создать пользователя (обязательный параметр). Группа должна существовать и быть типа user
	-g GROUPNAME	определить группу ОС, первичной для нового пользователя
	-G GROUPNAME1[,GROUPNAME2...]	определить список групп ОС, в который пользователь должен быть включен дополнительно
	-l [off|min|avg|max]	определить уровень детализации журнала accordx для нового пользователя
	-m [0|1|...|15]	определить уровень доступа субъекта
	-s [off|scrub_on_remove|...]	определить значения settings
	-c [off|set_time|...]	определить значения caps
	-T [path]	создание пользовательской учетной записи из шаблона. Из шаблона копируются только: acl, тип (user = 1), возможности пользователя (capabilities), настройки (settings), log_level, mand_level, флаг блокировки (blocked), разрешенные часы работы, static_icl, dynamic_icl (чтобы утилита не спрашивала интерактивно дополнительные данные - необходимо указать опции с паролем, данными для идентификации и именем группы в accordx). Значения из шаблона заменяются, если указаны соответствующие опции командной строки
	-f [path]	определить путь к БД accordx вместо указанного в конфиге
	-n	указание на то, что автоматически создавать

Команда	Опции/параметры команды	Комментарий
		пользователя в БД ОС не требуется (параметры -g, -G учитываться при этом не будут)
acx-admin user edit USERNAME		Редактировать пользователя (атрибуты пользовательской учетной записи) в БД accordx и в БД ОС (для изменения в БД ОС требуются права суперпользователя ОС)
	-N NEW_USERNAME	изменить имя пользователя
	-p PASSWORD	изменить пароль пользователя (влечет изменение xid)
	-t 'XX XXXXXXXXXXX XX'	изменить данные для идентификации (влечет изменение xid). Если изменились только данные для идентификации - дополнительно запрашивается пароль для пересчета xid
	-u UID	изменить UID пользователя (новый UID должен быть уникальный в ОС). При изменении UID права доступа в ОС на домашний каталог пользователя автоматически поменяются, для других файлов пользователя изменить права необходимо в ручном режиме
	-b [true|false]	задать флаг блокировки пользователя в accordx
	-w 'mon:XX:XX-XX:XX,XX:XX-XX:XX[;tue...]'	изменить разрешенные часы работы пользователя - можно задать пустое значение ''
	-a GROUPNAME	изменить группу accordx для пользователя. Группа должна существовать, быть типа user и пользователь должен быть уникальным в БД accordx
	-g GROUPNAME	изменить первичную группу ОС для пользователя
	-G GROUPNAME1[,GROUPNAME2...]	изменить список групп ОС, в который пользователь должен быть включен (если пользователь ранее был включен в группу, которой в списке нет - он более не будет входить в эту группу)
	-l [off|min|avg|max]	изменить уровень детализации журнала accordx для пользователя
	-m [0|1|...|15]	изменить уровень доступа субъекта
	-s [off|scrub_on_remove|...]	изменить значения settings
	-c [off|set_time|...]	изменить значения caps
	-f [path]	определить путь к БД accordx вместо указанного в конфиге
	-n	указание на то, что автоматически изменять пользователя в БД ОС не требуется (параметры -g, -G учитываться при этом не будут)
acx-admin user delete USERNAME		Удалить заданного пользователя из БД accordx и БД ОС (для изменения из БД ОС требуются права суперпользователя ОС)
	-d	force delete, удаление пользователя из БД ОС даже в случае если пользователь залогинен или к его файлам в данный момент обращается другой пользователь. Основная группа пользователя будет удалена, даже если является первичной для других пользователей
	-f [path]	определить путь к БД accordx вместо указанного в конфиге

Команда	Опции/параметры команды	Комментарий
	-n	указание на то, что автоматически удалять пользователя из БД ОС не требуется
acx-admin user show USERNAME		Просмотреть информацию о заданном пользователе с нужной степенью детализации выводимых атрибутов
	--verbose, -v	позволяют детализировать сообщения, выдаваемые при работе утилиты (например, раскрыть acl, icl)
	--mach, -m	позволяют формировать вывод в машиночитабельном формате (с использованием табуляции, без пробелов)
	-f <filename>	позволяет задать файл БД, отличный от файла БД в конфигурации acx-admin
acx-admin user	-h, --help (#./acx-admin user --help)	Опция для просмотра подробной справки

Примечание: Имя пользователя должно быть уникально во всей БД, пользователь может принадлежать только одной группе.

acx-admin shadow

acx-admin shadow - утилита для создания/удаления/редактирования учетных записей shadow в БД. Основные команды и опции данной утилиты описаны в таблице 4.

Таблица 4 - Основные команды и опции acx admin shadow

Команда	Опция/параметр команды	Комментарий
acx-admin shadow add SHADOWNAME		Создать shadow в БД accordx
	-b	установить атрибут blocked (по умолчанию при создании shadow blocked=false)
	-u UID	задать UID для учетной записи shadow
	-a ACXGROUP	задать группу, в которой необходимо создать shadow (группа должна существовать и быть типа shadow)
	-l <off|min|avg|max>	задать атрибут log_level
	-M <0|...|15>	задать атрибут mand_level
	-c <set_time|...>	задать атрибут settings
	-s <scrub_on_remove|...>	задать атрибут capabilities
	-f [path]	определить путь к БД accordx вместо указанного в конфиге
acx-admin shadow delete SHADOWNAME		Удалить shadow из БД accordx
	-f [path]	определить путь к БД accordx вместо указанного в конфиге
acx-admin shadow edit SHADOWNAME		Редактировать атрибуты shadow в БД accordx
	-N NEWSHADOWNAME	новое имя для субъекта
	-b <true|false>	изменить атрибут blocked
	-u UID	изменить UID для учетной записи shadow
	-a ACXGROUP	задать группу, в которую необходимо переместить shadow (группа должна существовать и быть типа shadow, из старой группы субъект удаляется)
	-l <off|min|avg|max>	изменить атрибут log_level

Команда	Опция/параметр команды	Комментарий
	-M <0|...|15>	изменить атрибут mand_level
	-c <set_time|...>	изменить атрибут settings
	-s <scrub_on_remove|...>	изменить атрибут capabilities
	-f [path]	определить путь к БД accordx вместо указанного в конфиге
acx-admin shadow show SHADOWNAME		Просмотреть информацию о shadow с нужной степенью детализации выводимых атрибутов
	--verbose, -v	позволяют детализировать сообщения, выдаваемые при работе утилиты (например раскрыть acl и другие атрибуты)
	--mach, -m	позволяют формировать вывод в машиночитабельном формате (с использованием табуляции, без пробелов)
	-f <filename>	позволяет задать файл БД, отличный от файла БД в конфигурации acx-admin
acx-admin shadow	-h, --help (#./acx-admin shadow --help)	Опция для просмотра подробной справки

acx-admin process

acx-admin process - утилита для создания/удаления/редактирования учетных записей process в БД accordx. Основные команды и опции данной утилиты описаны в таблице 5.

Таблица 5 - Основные команды и опции acx admin process

Команда	Опция/параметр	Комментарий
acx-admin process add		Создать process в БД accordx
	-b	установить атрибут blocked (по умолчанию при создании process blocked=false)
	-p <PATH>	задать путь до объекта файловой системы process (должен быть уникальным в БД) - обязательный параметр
	-a ACXGROUP	задать группу, в которой необходимо создать process (группа должна существовать и быть типа process) - обязательный параметр
	-l <off|min|avg|max>	задать атрибут log_level
	-M <0|...|15>	задать атрибут mand_level
	-c <set_time|...>	задать атрибут settings
	-s <scrub_on_remove|...>	задать атрибут capabilities
	-f [path]	определить путь к БД accordx вместо указанного в конфиге
acx-admin process delete		Удалить process из БД accordx
	-f [path]	определить путь к БД accordx вместо указанного в конфиге
acx-admin process edit		Редактировать атрибуты process в БД accordx
	-b <true|false>	изменить атрибут blocked
	-p <PATH>	изменить путь до объекта файловой системы process (должен быть уникальным в БД)

Команда	Опция/параметр	Комментарий
	-a ACXGROUP	задать группу, в которую необходимо переместить process (группа должна существовать и быть типа process, из старой группы субъект удаляется)
	-l <off|min|avg|max>	изменить атрибут log_level
	-M <0|...|15>	изменить атрибут mand_level
	-c <set_time|...>	изменить атрибут settings
	-s <scrub_on_remove|...>	изменить атрибут capabilities
	-f [path]	определить путь к БД accordx вместо указанного в конфиге
acx-admin process show		Просмотреть информацию о process с нужной степенью детализации выводимых атрибутов
	--verbose, -v	позволяют можно детализировать сообщения выдаваемые при работе утилиты (например раскрыть acl и другие атрибуты)
	--mach, -m	позволяют можно формировать вывод в машиночитабельном формате (с использованием табуляции, без пробелов)
	-f <filename>	позволяет задать файл БД, отличный от файла БД в конфигурации acx-admin
acx-admin process	-h, --help (#./acx-admin process --help)	Опция для просмотра подробной справки

acx-admin acl

acx-admin acl - утилита для работы с правилами разграничения доступа субъектов к объектам. Основные команды и опции данной утилиты описаны в таблице 6.

Таблица 6 - Основные команды и опции acx admin acl

Команда	Опция/параметр	Комментарий
show		Вывести на экран правила разграничения доступа или уровни доступа, при этом
	вызов '#acx-admin db show'	выводит краткую информацию (уровни конфиденциальности для всех объектов)
	--group,g <name>; --user,-u <name>; --shadow,-s <name>; --process,-p <name>	позволяют вывести правила разграничения доступа для конкретных субъектов (например 'объект доступа ~ доступные права на доступ к объекту')
	--verbose, -v	позволяют увеличивать детализацию вывода.
	--mach, -m	позволяют вывести информацию в удобном для выделения нужных значений (удобном для парсинга) виде (для отделения значений друг от друга используются символы табуляции \t и переноса строк \n).
	-f <filename>	позволяет задать файл БД, отличный от файла БД в конфигурации acx-admin.

Команда	Опция/параметр	Комментарий
add (формат команды № 1)1,		Добавить правила разграничения доступа[2], при этом:
	--verbose, -v или --quiet, -q	позволяют либо детализировать сообщения, выдаваемые при работе утилиты, либо скрыть их
	--group,g <name>; --user,-u <name>; --shadow,-s <name>; --process,-p <name>	позволяют задать субъекты, в чей список необходимо добавить правило разграничения доступа
	--recursion,-r <0|1|S>	позволяет задать уровень рекурсии для правила разграничения доступа (0 - только на текущий объект, 1 - на 1 уровень вложенности, если объект - каталог, S - рекурсивно на все поддиректории)
	-f <filename>	позволяет задать файл БД, отличный от файла БД в конфигурации acx-admin. В качестве параметра необходимо передать объект файловой системы, для которого будут применяться правила разграничения доступа. Примечание: для объекта файловой системы права доступа утилитой acx-admin можно задавать вне зависимости от его существования (например, при создании БД для других АРМ). Существование того или иного объекта, для которого задаются права доступа проверяется при загрузке БД в acx-core.
add (формат команды № 2)3		Задать уровень конфиденциальности для объекта доступа4, при этом:
	--verbose, -v или --quiet, -q	позволяют либо детализировать сообщения, выдаваемые при работе утилиты, либо скрыть их
	--recursion,-r <0|1|S>	позволяет задать уровень рекурсии для уровня конфиденциальности (0 - только на текущий объект, 1 - на 1 уровень вложенности, если объект - каталог, S - рекурсивно на все поддиректории)
	опция '-f <filename>'	позволяет задать файл БД, отличный от файла БД в конфигурации acx-admin. В качестве параметра необходимо передать объект файловой системы, для которого назначается уровень конфиденциальности
rm		Удалить правило разграничения доступа1.

1) Данный формат команды позволяет задать правила в рамках дискреционного контроля доступа, т.е. для каждого субъекта доступа (пользователя, shadow, process) необходимо явно задать разрешенные ему действия с каждым объектом доступа. Если правил для каких-то объектов явно не указано - любой доступ к ним будет запрещен.

2) В качестве параметра необходимо передать атрибуты доступа (RWXOCDNLMEnG)

3) Данный формат команды позволяет задать правила в рамках контроля доступа на основе иерархических меток, т.е. для каждого субъекта доступа (пользователя, shadow, process) явное указание на доступность того или иного объекта не указывается, каждому субъекту задается уровень доступа (при создании или редактировании), а каждому объекту - уровень конфиденциальности. В случае если уровень доступа субъекта выше или равен уровню конфиденциальности объекта - доступ разрешен, иначе - доступ запрещен.

4) В качестве параметра необходимо передать уровень конфиденциальности (от 0 до 15, 0 - наименьший уровень конфиденциальности).

Команда	Опция/параметр	Комментарий
		Примечание: Для изменения уровня конфиденциальности объекта необходимо выполнить acx-admin acl add (формат №2), задав новый уровень конфиденциальности.
	--verbose, -v или --quiet, -q	позволяют либо детализировать сообщения, выдаваемые при работе утилиты, либо скрыть их
	--group,g <name>; --user,-u <name>; --shadow,-s <name>; --process,-p <name>	позволяют задавать субъекты, у которых удаляется правило разграничения доступа
	--recursion,-r <0|1|S>	позволяет задать уровень рекурсии (0 - удалить только для текущего объекта, 1 - удалить на 1 уровень вложенности, S - удалить рекурсивно на все поддиректории)
	опция '-f <filename>'	позволяет задать файл БД, отличный от файла БД в конфигурации acx-admin
clear		Очистить списки правил разграничения доступа, при этом
	--verbose, -v или --quiet, -q	позволяют либо детализировать сообщения, выдаваемые при работе утилиты, либо скрыть их
	--group,g <name>; --user,-u <name>; --shadow,-s <name>; --process,-p <name>	позволяют задавать субъекты, чьи списки необходимо очистить
	-f <filename>	позволяет задать файл БД, отличный от файла БД в конфигурации acx-admin

acx-admin icl

acx-admin icl - утилита для редактирования списков контроля целостности (СКЦ, статического и динамического) для пользователей и групп. Основные команды и опции данной утилиты описаны в таблице 7.

Таблица 7 – Основные команды и опции acx admin icl

Команда	Опция/параметр	Комментарий
acx-admin icl add		Добавить объект в СКЦ группы или пользователя
acx-admin icl rm		Удалить объект из СКЦ группы или пользователя (по PATH или порядковому номеру)
acx-admin icl update		Пересчитать КЦ для объекта в СКЦ группы или пользователя (по PATH)
acx-admin icl clear		Очистить содержимое СКЦ (статического или динамического)
acx-admin icl		Вывести СКЦ пользователя или группы

1) В качестве параметра необходимо передать либо объект доступа, либо номер правила в списке ACL.

Команда	Опция/параметр	Комментарий
show		
	-h, --help (#./acx-admin icl --help)	Опция для просмотра подробной справки
	--verbose, -v или --quiet, -q	позволяют либо детализировать сообщения, выдаваемые при работе утилиты, либо скрыть их
	--mach, -m	позволяют формировать вывод в машиночитабельном формате (с использованием табуляции, без пробелов)
	-f <filename>	позволяет задать файл БД, отличный от файла БД в конфигурации acx-admin

Варианты использования acx-admin icl:

`#./acx-admin icl show [-v] [-m] [-g|-u <name>] [-f <filename>] [-s|-d]` - вывести статический/динамический СКЦ пользователя/группы

- опции -g, -u определяют, чей СКЦ выводить (пользователя или группы) и являются взаимозаменяемыми;
- опции -s, -d определяют, какой СКЦ вывести (динамический или статический) и являются взаимозаменяемыми.

`#./acx-admin icl add [-q|-v] [-g|-u <name>] [-f <filename>] [-s|-d] <PATH> [CHECKSUM]`

- опции -g, -u определяют субъект, которому необходимо добавить объект в СКЦ (пользователь или группа) и являются взаимозаменяемыми;
- опции -s, -d определяют, в какой СКЦ добавить объект и являются взаимозаменяемыми;
- PATH - полный путь до объекта файловой системы;
- CHECKSUM - контрольная сумма объекта.

`#./acx-admin icl update [-q|-v] [-g|-u <name>] [-f <filename>] [-s|-d] [PATH] [CHECKSUM]`

`#./acx-admin icl rm [-q|-v] [-g|-u <name>] [-f <filename>] [-s|-d] <PATH|OBJECT_NUMBER>`

`#./acx-admin icl clear [-q|-v] [-g|-u <name>] [-f <filename>] [-s|-d]`

acx-admin log

acx-admin log - утилита для работы с логами accordx. Основные команды и опции данной утилиты описаны в таблице 8.

Таблица 8 - Основные команды и опции acx admin log

Команда	Опция/параметр	Комментарий
acx-admin log		Просмотр содержимого log-файла

Команда	Опция/параметр	Комментарий
show		
acx-admin log stat		Вывод статистики log-файла
	-h, --help (#./acx-admin log --help)	Опция для просмотра подробной справки
	--verbose, -v или --quiet, -q	позволяют либо детализировать сообщения выдаваемые при работе утилиты, либо скрыть их.
	--mach, -m	можно формировать вывод в машиночитабельном формате (с использованием табуляции, без пробелов)
	-f <filename>	позволяет задать файл БД, отличный от файла БД в конфигурации acx-admin

Варианты использования acx-admin log:

`#./acx-admin log show [-v] [-m] [-C] <LOGFILE> - просмотреть содержимое log`

- опция -C позволяет вывести номер записи лога

`#./acx-admin log stat [-v] [-m] <LOGFILE>` - вывести статистику.

ПРИЛОЖЕНИЕ 3. Операции, регистрируемые подсистемой регистрации

Журнал регистрации «Аккорд-X K» содержит следующую информацию:

- порядковый номер события;
- дата и точное время регистрации события. Формат времени в журнале записывается в виде Unix (Posix) time - записываемое значение времени представляет собой количество секунд, прошедших с момента начала отсчета. Моментом начала отсчёта считается полночь (по UTC) с 31 декабря 1969 года на 1 января 1970;
- PID родительского процесса;
- PID процесса, который непосредственно осуществляет доступ (от имени пользователя - субъекта доступа);
- уровень детальности (min, avg, max - минимальный, средний, максимальный), установленной на момент регистрации события;
- класс события (proc, fs - события с процессами, с файловой системой);
- тип события – в таблице выводится краткая аббревиатура (подробное описание см. в таблице 9);
- результат – в таблице выводится краткая аббревиатура (подробное описание см. в таблице 10);
- тип субъекта, от имени которого осуществляется доступ (user, shadow, process);
- имя субъекта доступа (имя берется из БД Аккорд-X K);
- процесс, который осуществляет доступ от имени субъекта доступа (полный путь в ФС);
- объект доступа (полный путь в ФС). В таблице выводится полное наименование объекта доступа.

Таблица 9 - Типы событий, регистрируемые в журнале

Аббревиатура	Значение
Exec	запуск на выполнение
Mkdir	создание каталога
Chdir	переход в каталог
Rendir	переименование каталога
Rmdir	удаление каталога
Creat	создание объекта
Open	открытие объекта на чтение/запись
Close	закрытие объекта
Rename	переименование объекта
Link	создание ссылки на объект
Unlink	удаление ссылки на объект или удаление объекта, если количество жестких ссылок = 1
Setuid	смена uid
Login	идентификация и аутентификация пользователей
Logout	завершение сессии пользователя

Таблица 10 – Результаты операций, регистрируемые в журнале

Аббревиатура	Значение
Ok	все хорошо - событие не нарушило ПРД Аккорд-X K
Discr	доступ запрещен дискреционной политикой
Mand	доступ запрещен политикой на основе иерархических меток
Int	нарушена целостность объекта при контроле целостности динамического СКЦ
Err	произошла ошибка доступа в ОС

ПРИЛОЖЕНИЕ 4. Дополнительная настройка для пакетов acx-tmid-cards и acx-tmid-tokens

Требования для поддержки смарт-карт и токенов:

- необходимые зависимости: pcsc-lite ccid (как минимум). Для поддержки карт и считывателей ACS – libacsccid или соответствующие драйверы производителя, для поддержки карт и считывателей Athena – соответствующие драйверы производителя (http://www.athena-scs.com/support/software-driver-downloads#asedrive);
- необходимо добавить в файл конфигурации /usr/lib/pcsc/drivers/ifd-acsccid.bundle/Contents/Info.plist следующие значения:

```
<key>ifdVendorID</key>
<array>
      ...
>     <string>0x17e4</string>
>     <string>0x072f</string>
/array>

<key>ifdProductID</key>
<array>
      ...
>     <string>0x0040</string>
>     <string>0x90de</string>
</array>

<key>ifdFriendlyName</key>
<array>
      ...
>     <string>ACS ACR38U-CCID</string>
>     <string>ESMART TOKEN</string>
</array>
```

- необходимо добавить в файл конфигурации /usr/lib/pcsc/drivers/ifd-ccid.bundle/Contents/Info.plist следующие значения:

```
<key>ifdVendorID</key>
<array>
      ...
>     <string>0x24DC</string>
>     <string>0x24DC</string>
>     <string>0x0DC3</string>
>     <string>0x17E4</string>
>     <string>0x17E4</string>
>     <string>0x17E4</string>
>     <string>0x17E4</string>
>     <string>0x17E4</string>
>     <string>0x17E4</string>
```

```
>    <string>0x0529</string>
</array>
<key>ifdProductID</key>
<array>
     ...
>    <string>0x0101</string>
>    <string>0x100f</string>
>    <string>0x1004</string>
>    <string>0x0050</string>
>    <string>0x0051</string>
>    <string>0x0052</string>
>    <string>0x0053</string>
>    <string>0x0054</string>
>    <string>0x0055</string>
>    <string>0x0620</string>
</array>
<key>ifdFriendlyName</key>
<array>
     ...
>    <string>eToken</string>
>    <string>eToken</string>
>    <string>SmallReader</string>
>    <string>NXP Semiconductors SBI</string>
>    <string>NXP Semiconductors SBI</string>
>    <string>NXP Semiconductors SBI</string>
>    <string>NXP Semiconductors SBI</string>
>    <string>NXP Semiconductors SBI</string>
>    <string>NXP Semiconductors SBI</string>
>    <string>Etoken Pro Java</string>
</array>
```

В Н И М А Н И Е !

Процедуру добавления в файле конфигурации /usr/lib/pcsc/drivers/ifd-ccid.bundle/Contents/Info.plist следующих значений в секциях ifdVendorID, ifdProductID, ifdFriendlyName соответственно:

```
>    <string>0x0529</string>
>    <string>0x0620</string>
>    <string>Etoken Pro Java</string>
```

следует проводить только для ОС семейства RHEL, поскольку в более современных ОС идентификатор Etoken Pro Java прописан автоматически (входит в пакет ccid).

- Перезагрузить pcscd, выполнив /etc/init.d/pcscd restart.

ПРИЛОЖЕНИЕ 5. Типовой файл настроек печати пользователя

```
summary-company=User\ company
```

```
summary-phone=+7(495)500-00-05
printer=HP\ Color\ LaserJet\ 3800,1,2
```

ПРИЛОЖЕНИЕ 6. Типовой файл общих настроек печати

corner-print=true	печать углового штампа
corner-offsetx=0	смещение справа в угловом штампе
corner-offsety=0	смещение сверху в угловом штампе
corner-font-size=10	шрифт в угловом штампе
corner-line=true	печать линии в угловом штампе
corner-bold=false	жирный шрифт в уловом штампе
bottom-print=true	печать нижнего штампа
bottom-offsety=0	отступ снизу в нижнем штампе
bottom-font-size=12	шрифт в нижнем штампе
bottom-line=true	печать линии в нижнем штампе
bottom-align=middle	смещение в нижнем штампе
bottom-regnum-print=true	печать регистрационного номера
bottom-regnum-string=Уч\ №	формат строки с регистрационным номером
bottom-asname=AS	АС
bottom-docname-print=true	печать имени документа в нижнем штампе
bottom-date-print=true	печать даты в нижнем штампе
bottom-time-print=true	печать времени в нижнем штампе
bottom-access-print=true	печать грифа секретности в нижнем штампе
bottom-on-first=true	печать нижнего штампа на первой странице
pages-print=true	печать номер номера страниц
pages-top=true	номера страниц вверху
pages-on-first=true	нумерация с первой страницы
summary-print=true	печать итогового штампа
summary-computer-name-print=true	печать имени СВТ в итоговом штампе
summary-company=QQQ\ Company	печать названия компании в итоговом штампе
summary-phone=+7(495)444-33-22	печать телефона контактного лица в итоговом штампе
summary-regnum-print=true	печать регистрационного номера в итоговом штампе
summary-access-print=true	печать грифа секретности в итоговом штампе
summary-date-print=true	печать даты в итоговом штампе
summary-time-print=true	печать времени в итоговом штампе
summary-printer-print=true	печать имени принтера в итоговом штампе
summary-on-back=true	печать итогового штампа на обороте
change-access=false	возможность установки грифа пользователем

change-username=false	возможность изменения имени пользователя
change-docname=false	возможность изменения имени документа