ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
систем автоматизированного проектирования

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

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

РУКОВОДСТВО АДМИНИСТРАТОРА

37222406.26.20.40.140.085 90

Москва
2024

АННОТАЦИЯ

Настоящий документ является руководством администратора специального программного обеспечения средств защиты информации от несанкционированного доступа (СПО СЗИ НСД) «Аккорд-X K» (ТУ 509000-047-11443195-2011) (далее по тексту – СПО СЗИ НСД «Аккорд-X K», СПО «Аккорд-X K», «Аккорд-X K») и 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

В Н И М А Н И Е !

Перед началом установки комплекса «Аккорд-Х» рекомендуется подробно ознакомиться с эксплуатационной документацией на комплекс, прежде всего с «Описанием применения» (37222406.26.20.40.140.085 31) и настоящим Руководством.

1 ВВЕДЕНИЕ

Специальное программное обеспечение «Аккорд-X K» (ТУ 509000-047-11443195-2011), 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.

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-X K», 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 о 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» поддерживает работу под управлением следующих ОС Linux:

- CentOS 7;
- CentOS 8;
- Альт 9;
- Альт 10;
- Astra Linux Special Edition;
- Astra Linux Common Edition;
- Debian 7;
- Debian 10;
- Fedora 20;
- Fedora 24;
- OpenSUSE 12;
- OpenSUSE leap 42;
- Red Hat Enterprise Linux Server 6;
- Red Hat Enterprise Linux Server 7;
- Red Hat Enterprise Linux Server 8;
- Ubuntu 18;
- Р-Виртуализация Linux 7.5;
- РЕД ОС 7.1;
- РЕД ОС 7.2;
- РЕД ОС 7.3;
- TeNIX WS.

«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, pam_acx_passthrough.so);
- подсистема контроля печати (acx-print);
- модуль 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 K». В частности, к средствам администрирования СПО «Аккорд-X K» относятся следующие программы:

- утилиты настройки СПО «Аккорд-X K» acx-admin;
- утилиты установки ПРД пользователей acx-admin user, acx-admin group, acx-admin shadow, acx-admin acl;
- утилиты установки ПРД процессов acx-admin group, acx-admin acl;
- утилита работы с журналами регистрации событий acx-admin log.

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

2.1.2 Состав исполняемых модулей

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

пакет acx-admin - содержит утилиты администрирования СПО «Аккорд-X K» 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_passthrough.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 K (за исключением подсистемы контроля печати);

пакет acx-print - содержит модуль штатной подсистемы печати Linux CUPS, относящийся к ядру защиты СПО «Аккорд-X K».

Модуль acx-core.ko (МРД) является ключевым модулем в архитектуре Аккорд-X K - это ядро СПО Аккорд-X K, 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_passthrough.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-X K»

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

- применения парольного механизма;
- реализации механизмов разграничения доступа;
- контроля целостности критичных с точки зрения информационной безопасности программ и данных. В программной части СЗИ НСД возможна проверка целостности программ и данных по индивидуальному списку для отдельного пользователя, или группы пользователей. Подсистема контроля целостности предусматривает как статический список (проверка выполняется однократно в начале

[1] Данные об уровнях защищенности, обеспечиваемых СПО «Аккорд-X K», приведены в табл.1. ТУ 509000.047-11443195-2011

сеанса), так и динамический список, проверка по которому выполняется перед каждой загрузкой контролируемого файла в оперативную память;

- очистки внешней памяти;
- механизма регистрации действий пользователей в системном журнале, доступ к которому предоставляется только Администратору БИ.

2.3 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.

2.5 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»;
- организация установки СПО «Аккорд-Х К» и настройка его защитных средств в соответствии с установленными политиками разграничения доступа;
- эксплуатация СВТ с внедренным СПО «Аккорд-Х К», в т.ч., организация контроля над правильностью применения защитных механизмов СПО «Аккорд-Х К»;
- снятие защиты.

3 Установка и настройка СПО «Аккорд-Х К»

3.1 Общие сведения

Перед установкой и эксплуатацией СПО Администратор БИ проверяет соответствие комплектности условиям, заявленным в разделе «Комплектность поставки» Формуляра на СПО, сравнивает контрольные суммы файлов дистрибутива с указанными в Формуляре, после чего составляет организационно-распорядительный документ о вводе СПО в эксплуатацию и вносит сведения о нем в раздел Формуляра «Сведения о вводе в эксплуатацию и закреплении изделия».

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.

При необходимости полномочия Администратора БИ могут быть разделены на отдельные роли. Для реализации ролевого доступа необходимо ограничить соответствующие права пользователю root и выдать аналогичные права доступа другому пользователю, в том числе и в ОС. Так, если одному пользователю выдать права доступа только к файлу конфигурации и базе пользователей, а второму только к журналу - получится разделение административных полномочий, и первый будет Администратором БИ, а второй - Аудитором[2].

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;

[2] Далее по тексту предполагается, что функции аудитора выполняет Администратор БИ.

- механизма функционального замыкания программной среды пользователей средствами защиты СПО «Аккорд-Х К»;
- механизмов журналирования процедуры печати, управления процедурами ввода/вывода на отчуждаемые носители информации.

3.2 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;

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;

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

4. Реализация мер по безопасной настройке среды исполнения СПО «Аккорд-Х К», приведенных в Приложении 7 настоящего документа.

3.2.1 Установка СПО разграничения доступа

Первым шагом в процессе установки и настройки СПО разграничения доступа «Аккорд-Х К» является установка на жесткий диск СВТ СПО с дистрибутивного носителя, входящего в комплект поставки СПО «Аккорд-Х К».

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

```
# yum install acx-admin-1.3-1.x86_64.rpm
# yum install acx-core-0.6-1.x86_64.rpm
# yum install acx-tmid-usb-1.3-1.x86_64.rpm
... (здесь могут быть прочие пакеты для поддержки различных идентификаторов)
# yum install acx-gui-1.3-1.x86_64.rpm
# yum install acx-wui-1.3-1.x86_64.rpm
```

Либо для установки одновременно всех пакетов с помощью команды:

```
# yum install --skip-broken -y *.rpm
```

Для debian-based дистрибутивов это можно сделать, например, с помощью следующей команды (версия и разрядность устанавливаемых пакетов может отличаться):

```
# apt-get install ./acx-admin_1.3-4_amd64.deb ./acx-core_0.6-4_amd64.deb ./acx-tmid-usb_1.3-4_amd64.deb
```

Для извлечения файлов дистрибутива ОС TeNIX WS из архивов с расширением .tar.gz можно использовать команды

```
# cp acx-admin-1.3.tar.gz acx-core-1.3.tar.gz acx-tmid-usb-1.3.tar.gz /
# cd /
# tar xf acx-core-1.3.tar.gz
# tar xf acx-admin-1.3.tar.gz
# tar xf acx-tmid-usb-1.3.tar.gz
```

При этом для работы ПО acx-tmid-usb следует вручную установить зависимости командой

```
# tpkg pcsc-lite
```

В Н И М А Н И Е !

Некоторые ОС Linux в рамках одной версии имеют не только несколько разных ядер, но и десятки сборок, поэтому при установке версии дистрибутива Аккорд-X K для Вашей ОС, но для другой сборки, модули могут установиться некорректно. В этом случае после перезагрузки ОС будет загружена, а модули Аккорд-X K - нет. В связи с этим рекомендуется:

1) не настраивать PAM-модуль до перезагрузки и проверки успешности установки Аккорд-X K;
2) в случае, если после перезагрузки модули Аккорд-X K не загрузились, обратиться в службу техподдержки и получить пакет для конкретной сборки.

В Н И М А Н И Е !

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).

В Н И М А Н И Е !

Для некоторых дистрибутивов (из известных случаев – Debian 7.6.0 x64, Astra Linux SE 1.3 x64, Ubuntu 18.04.3 x64) после установки «Аккорд-X» и при попытке запуска любой утилиты типа acx-admin выводятся сообщения об отсутствии динамических библиотек «Аккорд-X». Это связано с тем, что такие дистрибутивы их не видят из-за специфических настроек линковщика, и для решения данной проблемы следует либо перенести библиотеки, располагаемые по пути /usr/lib64/, в каталог /usr/lib/, либо создать на них ссылки. Пример скрипта, решающего описанную проблему:

```
#!/bin/bash
```

```
libs=(          "/lib64/security/pam_acx_local.so" \
        "/lib64/security/pam_acx_remote.so" \
        "/usr/lib64/libacx-core.so*" \
        "/usr/lib64/tmid-accord.so" \
        "/usr/lib64/tmid-acos3-apdu.so" \
        "/usr/lib64/tmid-acos5-apdu.so" \
        "/usr/lib64/tmid-laser-apdu.so" \
        "/usr/lib64/tmid-mifare-apdu.so" \
        "/usr/lib64/tmid-mifarek-apdu.so" \
        "/usr/lib64/tmid-mifare_desfire-apdu.so" \
        "/usr/lib64/tmid-shipka.so" \
        "/usr/lib64/libosci.so*" \
        "/usr/lib64/tmid-etoken-apdu.so"
        "/usr/lib64/tmid-etoken_pro-apdu.so"
        "/usr/lib64/tmid-etoken_pro_java-apdu.so"
        "/usr/lib64/tmid-rutoken-pkcs11.so"
        "/usr/lib64/tmid-tm-usb.so" \
        "/usr/lib64/libacx-db.so*" \
        "/usr/lib64/libacx-log.so*" \
        "/usr/lib64/libtmid.so*" \
        "/usr/lib64/libccid_dev.so" \
        "/usr/lib64/libpkcs11_dev.so" \
        "/usr/lib64/libtmid_utils.so" \
        "/usr/lib64/cups/filter/accord.cnf" \
        "/usr/lib64/cups/filter/accord.users/user.cnf" \
        "/usr/lib64/libacx-print.so*" \
        )

for lib in `ls ${libs[@]} 2>/dev/null`
do
 path=`echo $lib | sed 's/64//g'`
 # if files from $libs exists, then create symbolic links for them
 if [ -e $lib ]; then
        # first unlink previous links
        if [ -e $path ]; then
                unlink $path
        fi
        echo "${lib}: exists, creating link in ${path}"
```

```
        ln -s $lib $path
    fi
    done

    echo "Configuring library paths successfully ended."
    exit 0
```

В Н И М А Н И Е !

В Ubuntu 18.04.3 PAM-модули установлены в /lib/x86_64-linux-gnu/security/, а не в /lib/security (что пытается исправить скрипт из предыдущего блока "ВНИМАНИЕ!").

В соответствии с этим, нужно либо создать вручную ссылки с помощью команд

```
ln -s /lib64/security/pam_acx_local.so /lib/x86_64-linux-gnu/security/
ln -s /lib64/security/pam_acx_remote.so /lib/x86_64-linux-gnu/security/
```

либо при настройке PAM (раздел 3.4.9) использовать абсолютный путь до соответствующего PAM-модуля, например, в /etc/pam.d/common-auth:

```
auth requisite /lib64/security/pam_acx_local.so password tmid_timeout=2 debug
auth [success=1 default=ignore] pam_unix.so nullok_secure try_first_pass
```

В Н И М А Н И Е !

При работе в ОС TeNIX WS следует изменить предустановленный графический менеджер входа в систему sddm на пакет lightdm. В качестве примера можно использовать команды

```
tpkg lightdm lightdm-gtk-greeter
tpkg -i lightdm
systemctl disable sddm
systemctl enable lightdm
```

или обратиться к документации разработчика ОС TeNIX WS.

3.2.2 Начальная конфигурация СПО «Аккорд-Х К»

После выполнения процесса установки СПО разграничения доступа необходимо провести начальную конфигурацию с помощью утилиты **acx-config** (входит в состав пакета **acx-admin - acx-admin config**). Для автоконфигурирования следует выполнить команду:

```
# acx-config create
```

В Н И М А Н И Е !

Здесь и далее – для получения справки и описания для той или иной утилиты необходимо либо запустить ее без указания каких-либо опций, либо использовать опции -h, --help

```
[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 К», включение дискреционной политики разграничения доступа

В результате выполнения приведенной команды в /etc/accordx/acx-config.json создастся конфигурационный файл для «Аккорд-X К» вида (см. также рисунок 1):

```
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 комплекса. 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 записи «вниз» в политике разграничения доступа на основе иерархических меток;
   - soft-mode – включить мягкий режим;
   - mpl – включить контроль точек монтирования;
   - icl – включить контроль целостности;
   - 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).

В Н И М А Н И Е !

При работе в ОС TeNIX WS после распаковки пакетов с ПО следует выполнить вручную ряд команд. Примеры некоторых команд:

- mkdir -p /etc/accordx /var/log/accordx/
- acx-admin config create
- acx-admin db create –c
- chmod g+s /var/log/accordx/
- systemctl daemon-reload
- systemctl enable acx
- systemctl disable acx
- /sbin/depmod -a

3.2.3 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`

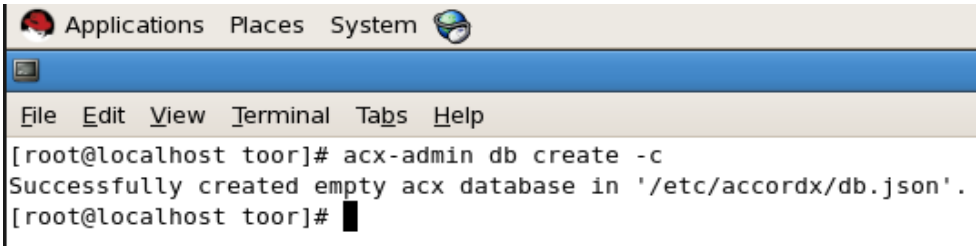

Рисунок 2 – Создание базы данных пользователей на основе конфигурационного файла

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

В Н И М А Н И Е !

Чтобы в процессе дальнейшего функционирования «Аккорд-Х К» можно было выполнить вход в ОС в качестве Администратора БИ (суперпользователя; пользователя root), после создания базы данных пользователей для него необходимо назначить идентификатор и задать пароль в БД (данную процедуру необходимо выполнить потому, что при создании БД использовалась опция автосоздания нужных по умолчанию пользователей, и, следовательно, идентификатор и пароль для пользователя root еще не заданы). См. рисунок 4.

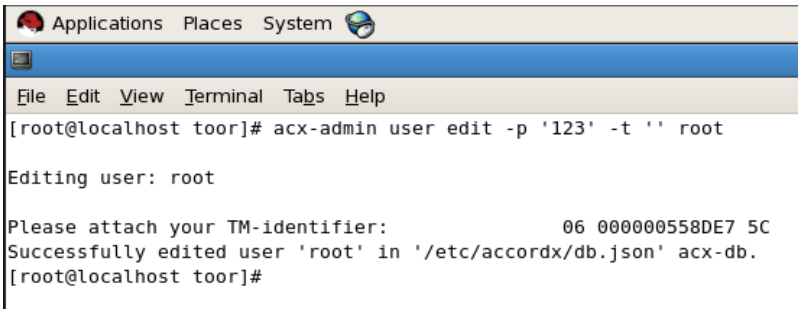

Рисунок 4 – Назначение персонального идентификатора и задание пароля для пользователя root

3.2.4 Создание групп пользователей

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

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

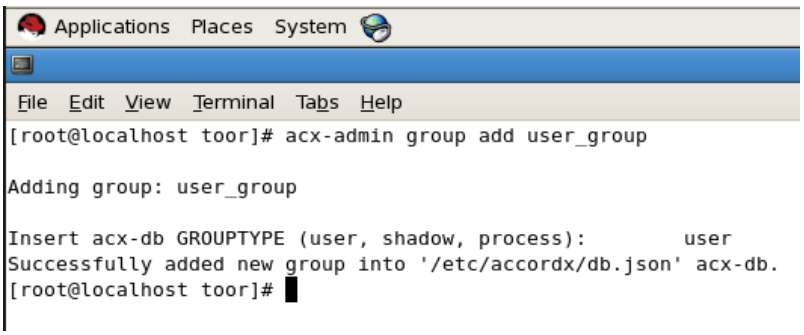

Рисунок 5 – Создание группы пользователей

На данный момент группирование пользователей не оказывает влияния на общую работу комплекса – группы используются для удобства. Однако

необходимо учитывать, что для корректной работы комплекса 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 комплекса на раннем этапе загрузки ОС (т.е. до появления в системе реального пользователя), в соответствии с этим дискреционные ПРД и ПРД на основе иерархических меток 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 «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 идентификатор и пароль (см. рисунок 5).

3.2.5 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 дискреционные ПРД и ПРД на основе иерархических меток с помощью утилиты **acx-admin-log** (командой `# acx-admin log makerights` ...).

Создадим, например, обычного пользователя с именем toor (рисунок 6):

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

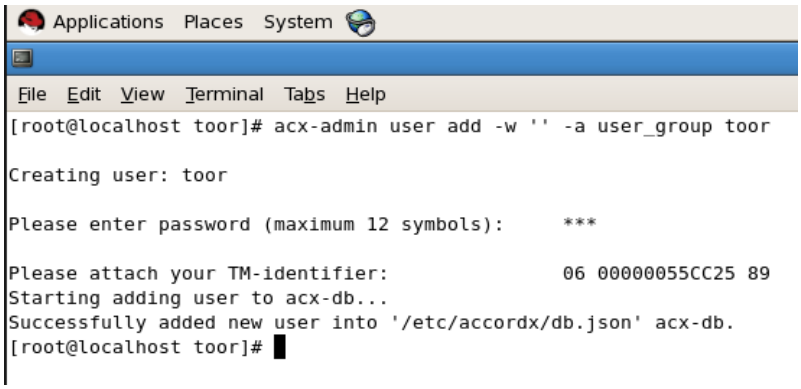

Рисунок 6 – Создание обычного пользователя с именем toot

После выполнения описанной последовательности действий пользователь с именем toor появляется в базе данных пользователей «Аккорд-X K».

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

ВНИМАНИЕ!

При создании или редактировании пользователей необходимо удостовериться, что uid и пароль реальных пользователей, создаваемых в БД «Аккорд-X K», совпадают со значениями из файла /etc/passwd. Иначе произвести операцию login данным пользователем не получится. Если пользователь, создаваемый в «Аккорд-X K», 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 комплекса 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).

3.2.6 Задание дискреционных прав разграничения доступа

Рассмотрим вопрос задания ПРД для созданных пользователей «Аккорд-X K». Однако стоит иметь ввиду, что при установке «Аккорд-X K» впервые желательно пропустить следующие пункты с настройкой ПРД/контроля целостности и закончить процесс установки СПО «Аккорд-X K» (чтобы убедиться, что комплекс работоспособен с отключенными механизмами безопасности или с ПРД, разрешающими все действия).

Итак, после успешного выполнения установки и первичной настройки СПО необходимо задать дискреционные политики разграничения доступа созданным пользователям с помощью утилиты **acx-admin acl**.

В СПО «Аккорд-X K» 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;

C - создание объекта;

D - удаление объекта;

N - переименование объекта;

L - создание жесткой ссылки для объекта

M - создание каталога;

E - удаление каталога;

n – переименование каталога.

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).

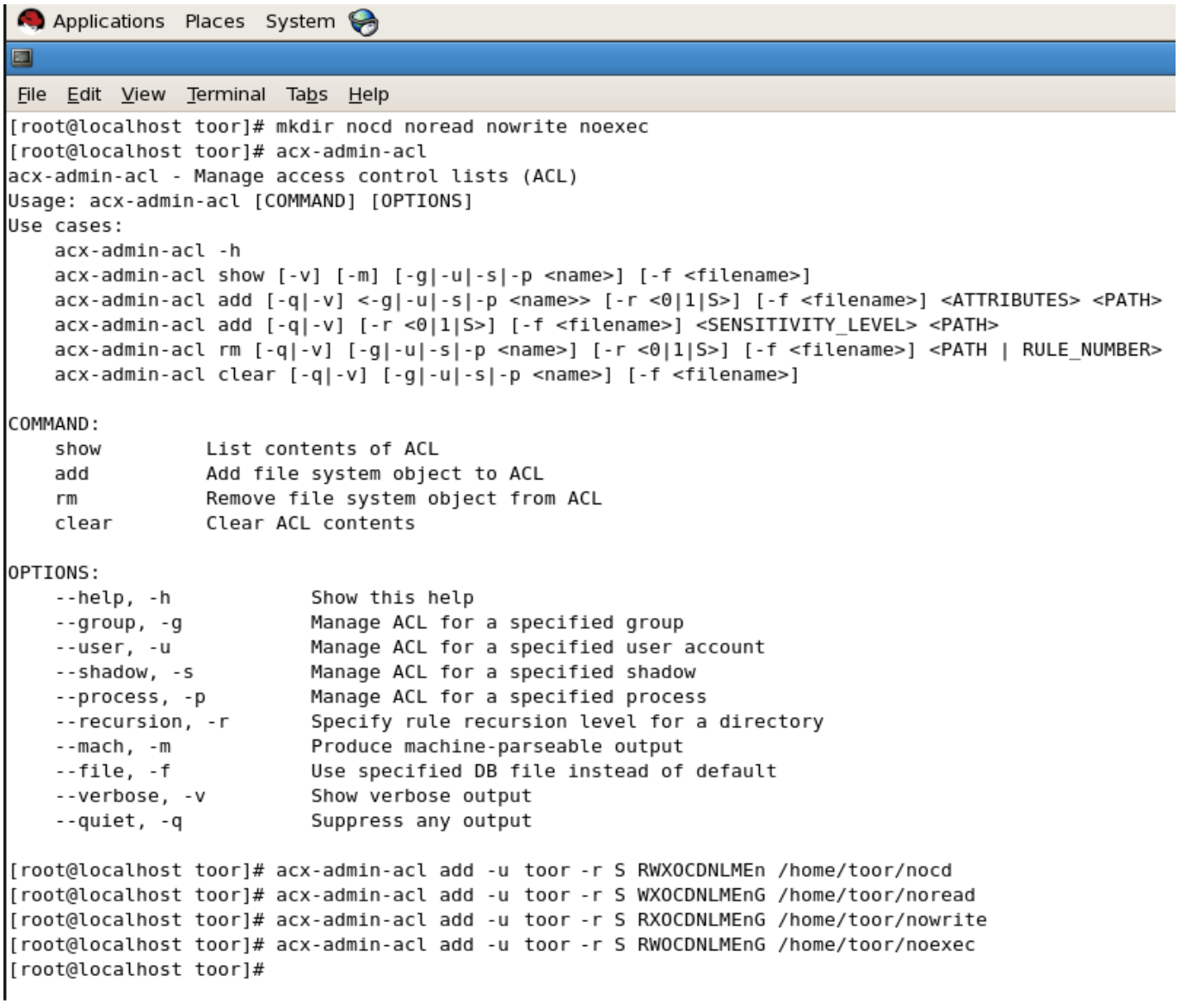

Рисунок 8 – Задание дискреционной политики безопасности

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/**", "RXOCDNLMEnG"]]
```

3.2.7 Задание иерархических меток и уровней доступа

Задать иерархические метки для объектов файловой системы и уровни доступа на их основе 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 4.2.6 и 4.2.7 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-*`).

3.2.8 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.

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).

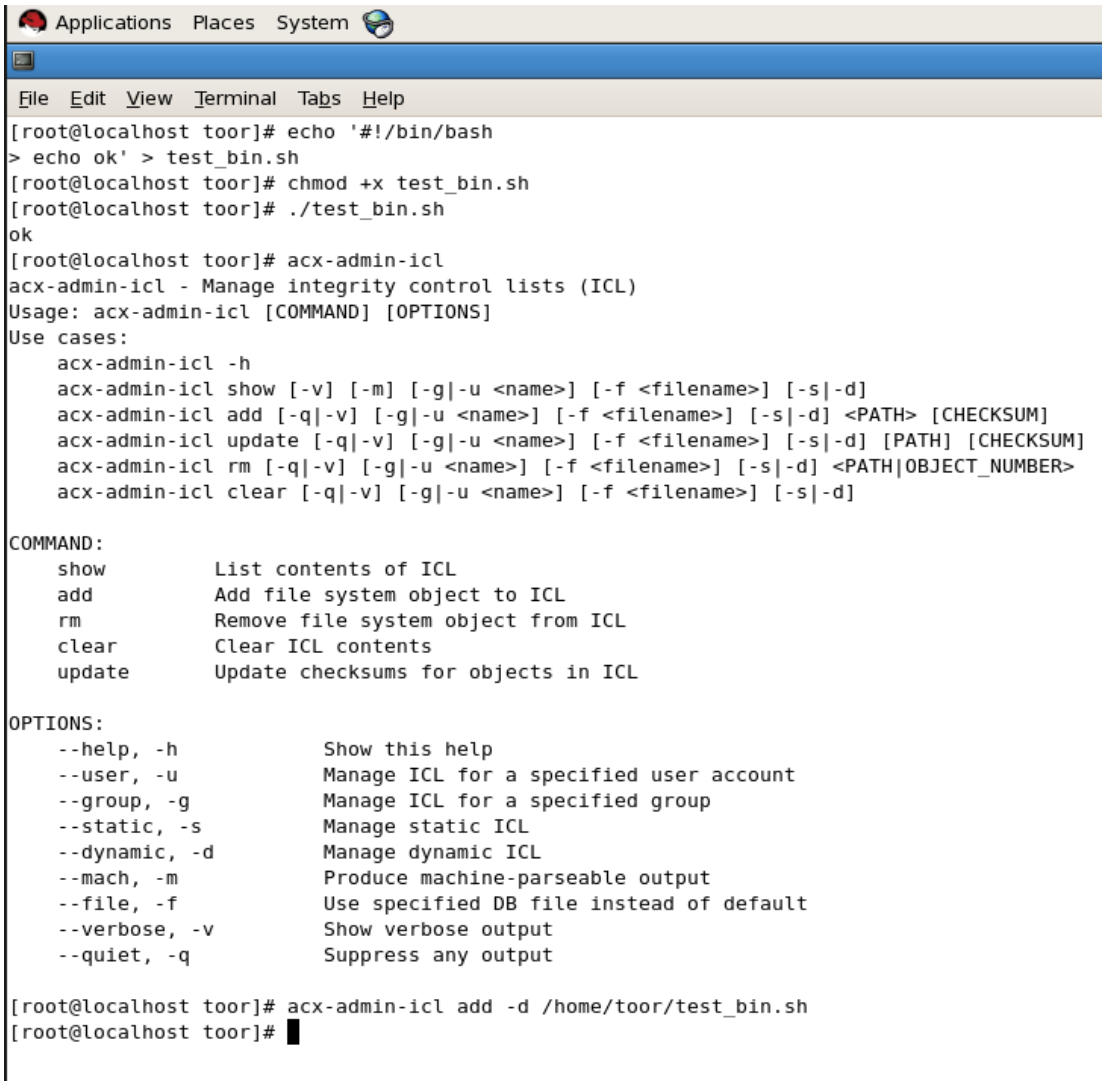

Рисунок 9 – Создание и занесение в динамический СКЦ бинарного файла

Только что добавленный объект в динамическом СКЦ выглядит следующим образом:

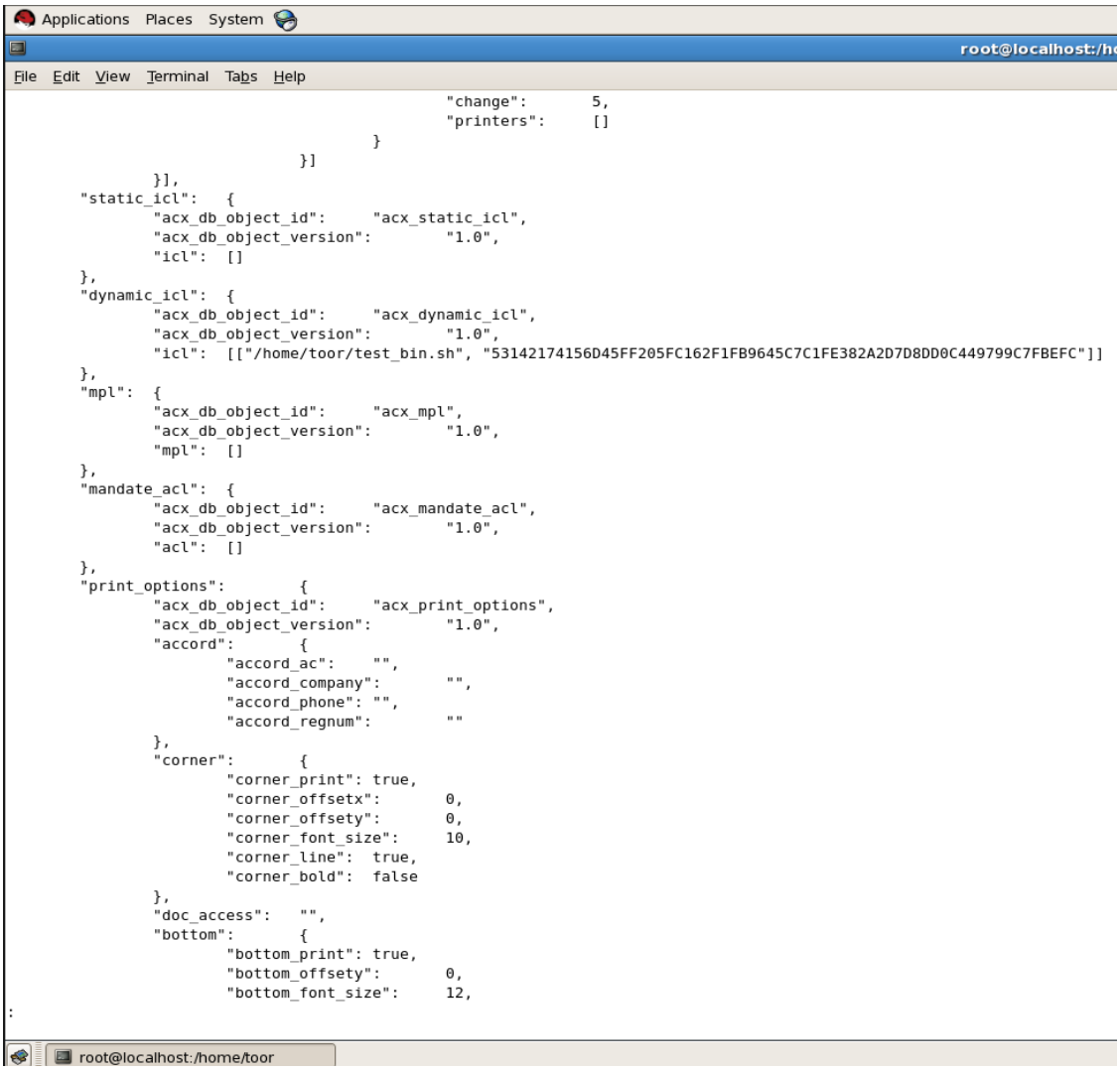

Рисунок 10 – Демонстрация добавленного в динамический СКЦ объекта

Статический контроль целостности

Статический контроль целостности осуществляет контроль целостности любых файлов в тот момент, когда запускается утилита **acx-integrity-controller/acx-integrity-controller-db**. Объекты для статического СКЦ необходимо добавлять для БД – т.е. в `db->static_icl`.

Рекомендуется осуществлять статический контроль целостности ядром комплекса. Для включения статического контроля целостности PAM-модулю pam_acx_local.so нужно дописать опцию icl через пробел:

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

В случае нарушения целостности файлов из статического СКЦ доступ в систему возможен только пользователю с именем root (т.е. суперпользователю).

ВНИМАНИЕ!

В СПО «Аккорд-Х К» по умолчанию установлена политика задания изначально разрешительных правил разграничения доступа (когда изначально всем пользователям в системе все разрешено, а не запрещено). Для задания

разрешительных ПРД в файле конфигурации ПАК «Аккорд-X» существует опция permissive-acl.

ВНИМАНИЕ!

В случае реализации разрешительных ПРД для политики на основе иерархических меток необходимо для пользователя типа shadow с именем root устанавливать минимальный уровень доступа (clearance в 0), иначе загрузиться при такой настройке не получится (для shadow root будет недоступна "запись вниз" в объекты с низким уровнем конфиденциальности, т.к. при "разрешительной" политике считается, что все объекты, не перечисленные в БД «Аккорд-X K», имеют уровень конфиденциальности 0).

ВНИМАНИЕ!

В случае реализации политики задания изначально запретительных ПРД (когда опция permissive-acl установлена в значение false) 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 «Аккорд-X K» 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).

3.2.9 Настройка PAM

Для корректного входа в ОС пользователей по идентификаторам и регистрации их в мониторе разграничения доступа необходимо корректным образом настроить[3] PAM в ОС Linux. Только при выполнении этого условия ядро СПО 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 «Аккорд-X K», 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 идентификатора и пароля осуществляет PAM, проверку производного от идентификатора и пароля значения осуществляет сам монитор по своей БД).

Следует обратить внимание, что в различных версиях и дистрибутивах ОС Linux конкретные сценарии и названия PAM-модулей могут отличаться, в связи

[3)] Настройка PAM выполняется только в командной строке

с чем в данном описании лишь показан принцип, в соответствии с которым необходимо настраивать PAM.

PAM в ОС Linux представляет собой набор модулей аутентификации, которые физически располагаются в /lib/security[4] (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-X K» 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-X K».

Рассмотрим настройку PAM на следующем примере:

1. 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.

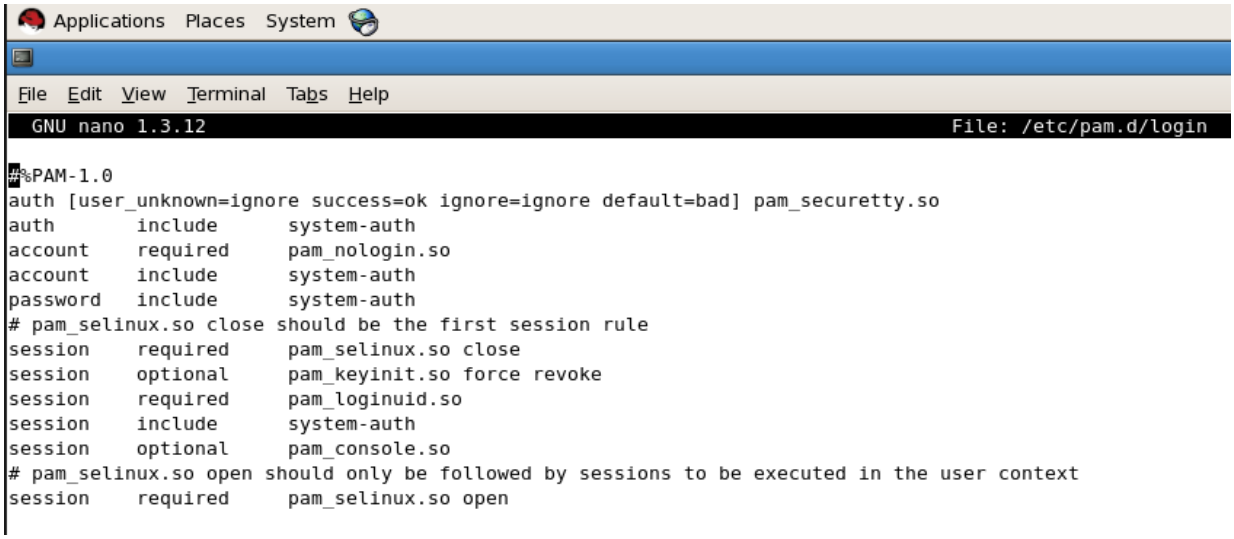

Рисунок 11 – Утилита login

2. 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
```

[4] В некоторых 64-разрядных дистрибутивах – /lib64/security

```
auth        requisite       pam_succeed_if.so uid >= 500 quiet
...             ...             ...
```

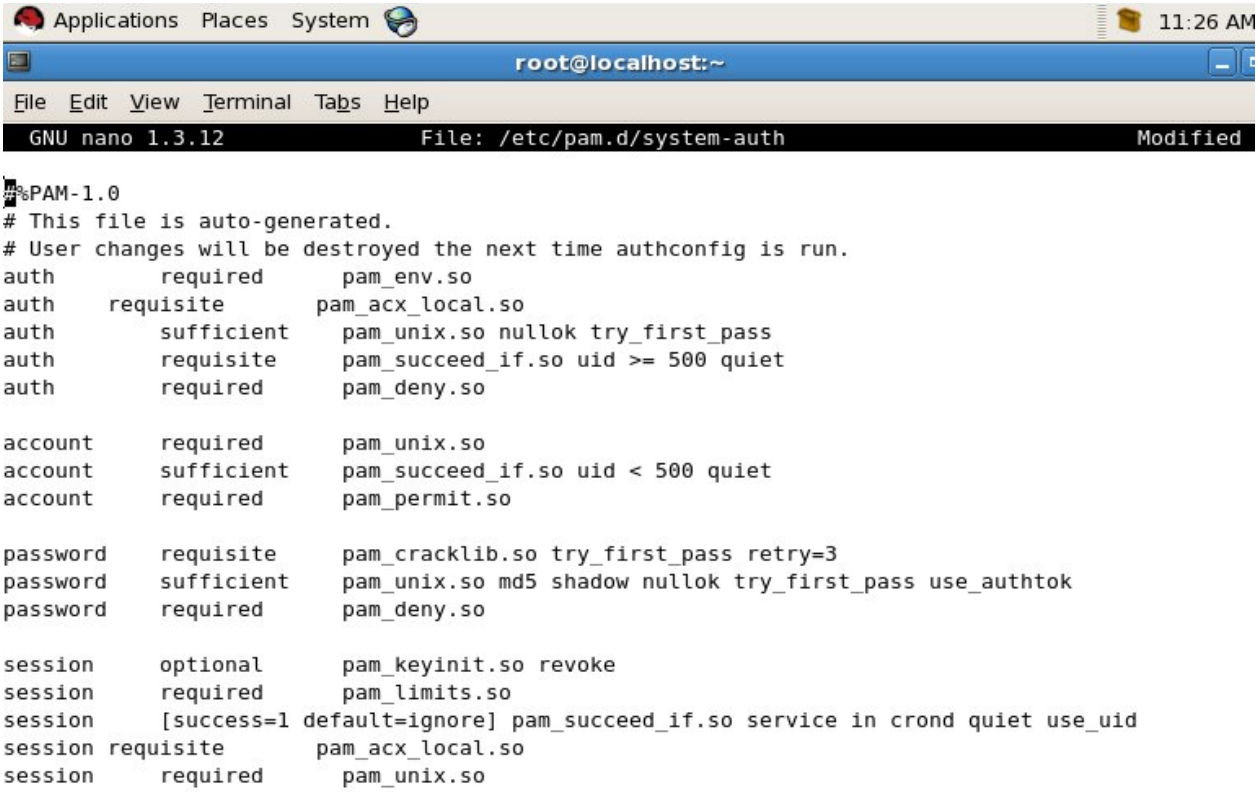

Рисунок 12 – Сценарий system-auth

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.

3. В /etc/pam.d/system_auth зададим наш PAM-модуль **pam_acx_local.so** дополнительно к стандартному модулю, 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
...             ...             ...
```

При этом для pam_unix.so обязательно должна быть указана опция try_first_pass (в некоторых дистрибутивах Linux она отсутствует).

4. 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). В некоторых ситуациях 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.

5. Аналогичным образом можно настроить сценарии для GUI – **gdm/kdm/xdm**, а также прочих утилит (часто это /etc/pam.d/password-auth и /etc/pam.d/system-auth).

Применяя описанные выше рассуждения для секции auth, аналогично PAM-модуль «Аккорд-X K» 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 K», соответствуют паролям пользователей ОС.

PAM-модули «Аккорд-X K» 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» 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 K») необходимо внести в конец файла /etc/sudoers 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.

В Н И М А Н И Е !

В СПО «Аккорд-Х К» предусмотрена возможность удаленного подключения к ПК с установленным «Аккорд-Х К» с использованием аппаратных идентификаторов при использовании вместо pam_acx_local.so модуля pam_acx_remote.so, который позволяет подключаться к ПК с «Аккорд-Х К» удаленно по протоколам ssh и telnet.

На ПК с «Аккорд-Х К» нужно настроить, например, /etc/pam.d/sshd: вставить pam_acx_remote.so аналогично pam_acx_local.so, но при этом создать копии всех файлов цепочек @include из /etc/pam.d/sshd, чтобы локальная аутентификация продолжала работать с pam_acx_local.so.

На клиентском ПК с Linux, с которого предполагается подключаться удаленно к ПК с «Аккорд-Х К», установить пакеты acx-remote (для подключения по ssh дополнительно требуется утилита sshpass) и acx-tmid-* для поддержки соответствующего типа идентификаторов.

После этого можно подключаться к ПК с «Аккорд-Х К» удаленно по ssh, выполняя команду acx-remote (помощь выводится при запуске без параметров). Предварительно необходимо подтвердить ключ хоста с помощью стандартного ssh клиента.

Аналогично можно настроить вместо ssh подключение по telnet (для /etc/pam.d/telnetd, вместо утилиты sshpass требуется expect).

В случае использования идентификации и аутентификации без аппаратных идентификаторов (по логину и паролю) указанные выше пакеты не требуются. На ПК с «Аккорд-Х К» необходимо установить обычный пакет acx-core (и использовать pam_acx_local.so), а на клиентском ПК использовать стандартное ПО для удаленного подключения.

3.2.10 Настройка запуска монитора разграничения доступа

На последнем шаге настройки необходимо обеспечить запуск монитора разграничения доступа на раннем этапе загрузки системы[5] (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:

1. 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
```

2. Распаковать созданную копию initrd с помощью скрипта из пакета **acx-core** (рисунок 13)**:**

[5] Данная настройка выполняется только в командной строке

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

3. 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). При этом следует иметь в виду, что «cp /lib/acx-core.ko .initrd-tmp/fs/lib/» в 64-разрядных ОС имеет вид «cp /lib64/acx-core.ko .initrd-tmp/fs/lib/».

```
# 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
```

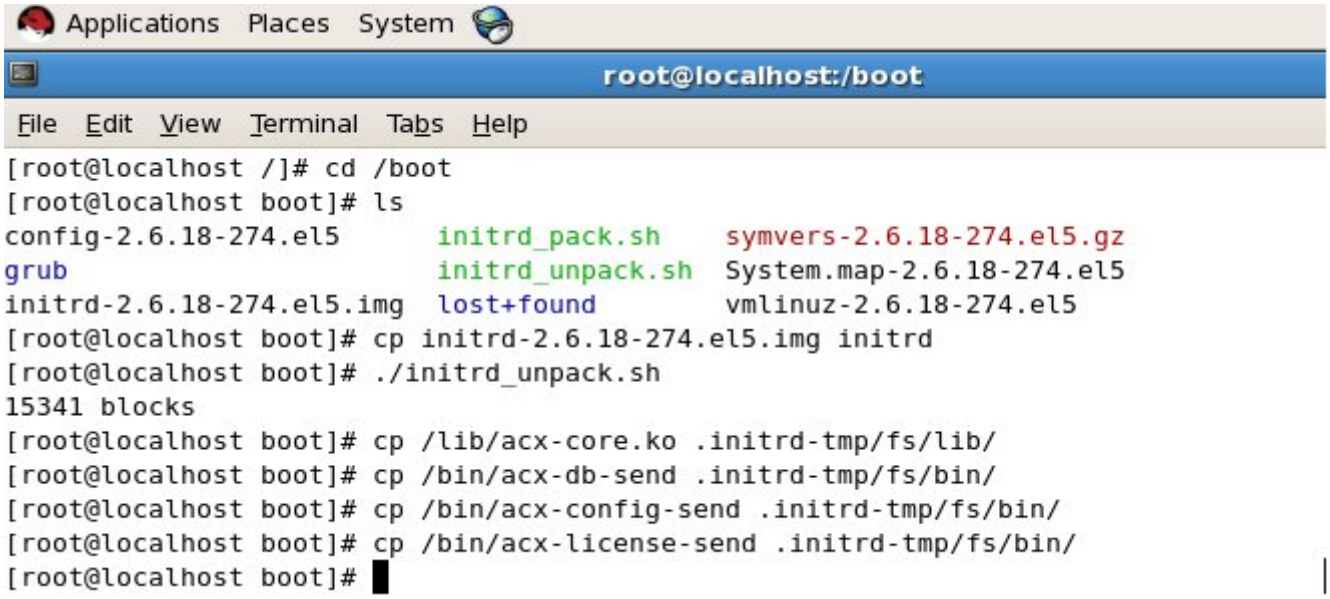

Рисунок 13 – Настройка образа начальной загрузки

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

```
#################################################################
#echo "Loading Accord-AMDZ drivers"
#/sbin/insmod /lib/accord-le.ko
#/sbin/insmod /lib/tmdevice.ko

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
#################################################################
```

При этом следует учитывать, что в некоторых ОС путь может отличаться: вместо **/sysroot** может быть **/root**. Это зависит от пути, объявленного выше в скрипте init.

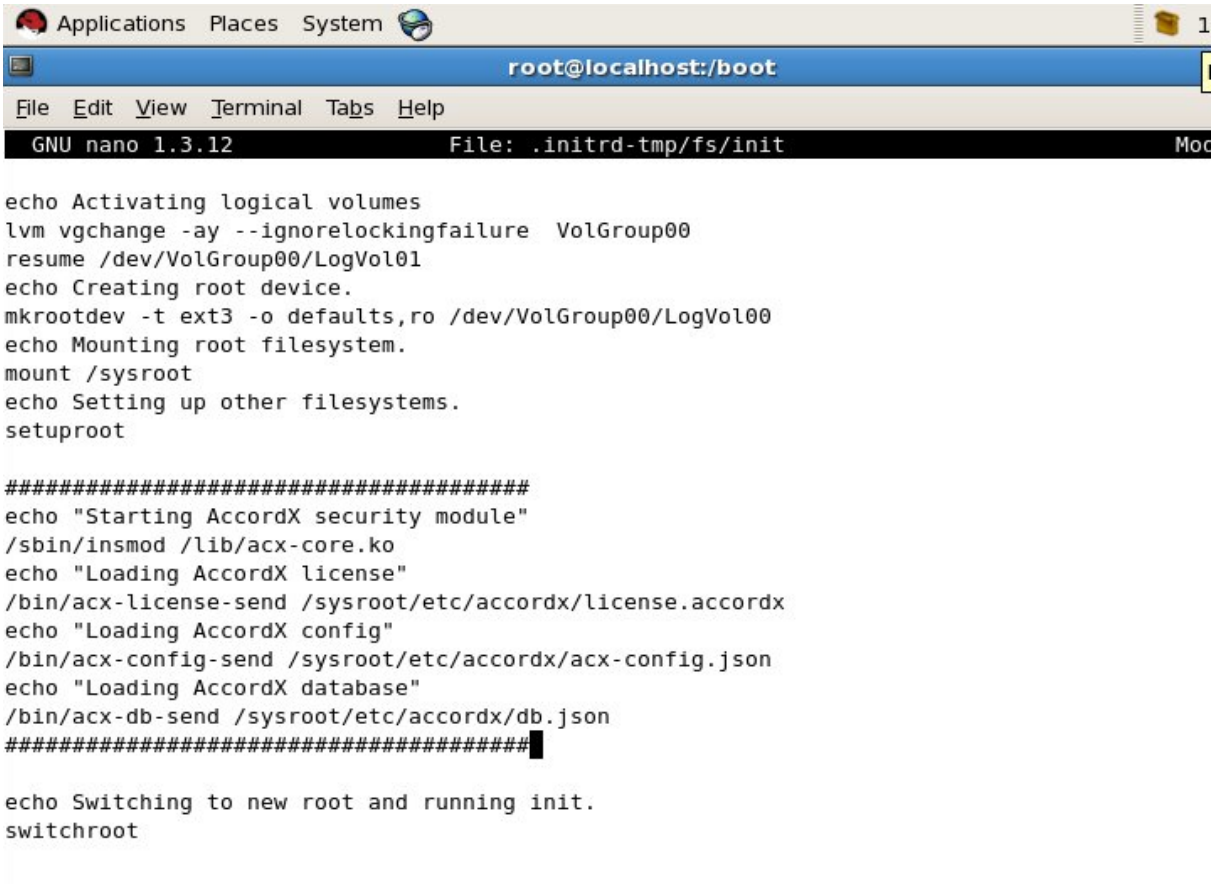

Рисунок 14 – Информация о загрузке монитора РД в скрипте init

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).

В Н И М А Н И Е !

Для ОС RHEL/CentOS версии 7 и выше, а также всех systemd-based дистрибутивов необходимо иначе встраивать компоненты в initrd (вместо прописывания сценариев в .initrd-tmp/fs/init). Для этого нужно либо применить патч-файл, содержимое которого приведено ниже, либо внести изменения из него самостоятельно, дополнительно выставив права на выполнение для файла /boot/.initrd-tmp/fs/bin/startacx.

Для Ubuntu 18.04.* для корректного входа в графическую среду gdm3 нужно использовать экспериментальный параметр gui_gdm3_setuid, полный список необходимых параметров acx-core.ko для этой ОС - "gui_allow_setuid=1 gui_gdm3_setuid=1

Содержимое патч-файла rhel-centos-7-initrd.patch:

```
--- .initrd-tmp.orig/fs/bin/startacx    1970-01-01 03:00:00.000000000 +0300
+++ .initrd-tmp/fs/bin/startacx   2017-04-25 11:04:45.103038612 +0300
@@ -0,0 +1,16 @@
+#!/bin/bash
+
+#####################################################################
+#echo "Loading Accord-AMDZ drivers"
+#/sbin/insmod /lib/accord-le.ko
+#/sbin/insmod /lib/tmdevice.ko
+
+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
+#####################################################################
--- .initrd-tmp.orig/fs/usr/lib/systemd/system/initrd-switch-root.service 2017-04-25 10:51:28.929379390 +0300
+++ .initrd-tmp/fs/usr/lib/systemd/system/initrd-switch-root.service      2017-04-25 11:07:42.483408273 +0300
@@ -16,5 +16,7 @@ AllowIsolate=yes
 [Service]
 Type=oneshot
 # we have to use "--force" here, otherwise systemd would umount /run
+ExecStart=
+ExecStart=/bin/startacx
 ExecStart=/usr/bin/systemctl --no-block --force switch-root /sysroot
 KillMode=none
```

5. Запаковать образ initrd с помощью скрипта из пакета **acx-core:**

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

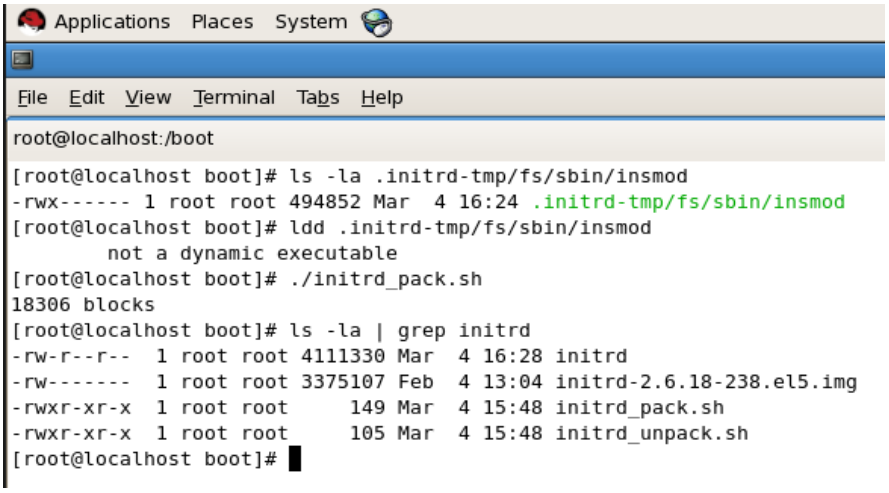

Рисунок 15 – Проверка наличия файла insmod, запаковка образа initrd

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

ВНИМАНИЕ!

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.

ВНИМАНИЕ!

Необходимо удостовериться в наличии корректного исполняемого файла .initrd-tmp/fs/sbin/insmod (со всеми зависимостями относительно каталога .initrd-tmp/fs/, перечисленными при выполнении "ldd .initrd-tmp/fs/sbin/insmod").

3.2.11 Настройка загрузки файла initrd

Теперь для запуска ОС вместе с монитором разграничения доступа необходимо прописать[6] полученный файл initrd для автовыбора в загрузчике (рассмотрен загрузчик grub) вместо [current initrd] (рисунок 16).

[6)] Данная процедура выполняется только в командной строке

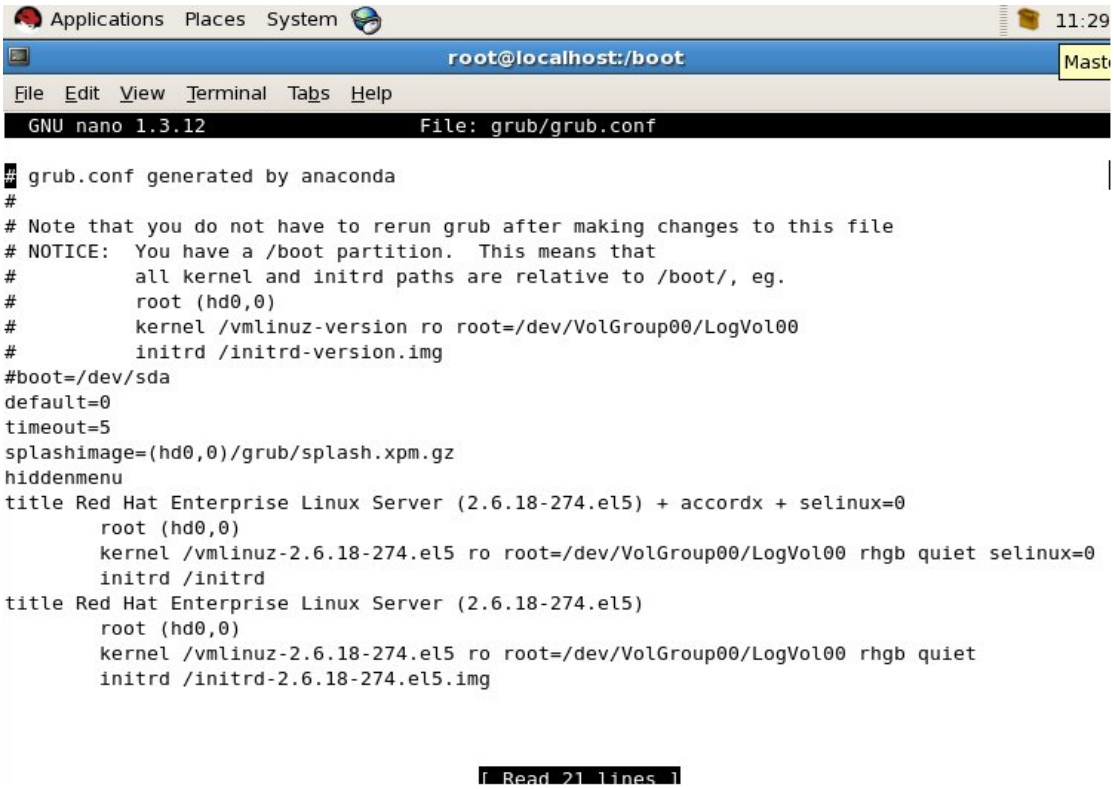

Рисунок 16 – Файл initrd прописан для автовыбора в загрузчике grub

ВНИМАНИЕ!

В приведенном примере показан конфигурационный файл загрузчика grub в момент настройки СПО «Аккорд-X K». По окончании настройки (перед вводом СПО «Аккорд-X K» 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-X K»);

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).

3.2.12 Контроль доступа к информации на внешних устройствах

Для корректной взаимосвязи 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 устройства. 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-X 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 – все зависит от решаемых задач по контролю за внешними носителями информации.

3.2.13 Активизация подсистемы разграничения доступа к ресурсам ПЭВМ

После выполнения описанной выше последовательности действий по установке и настройке комплекса необходимо выполнить активацию подсистемы разграничения доступа, скопировав файл лицензии в корневой каталог /etc/accordx. Этот файл потребуется при старте ОС с новым initrd.

Запросить файл лицензии[7] может пользователь с правами root (получить права – команда su или sudo). Далее следует выполнить команду dmidecode > dmidecode.list. Полученный файл dmidecode.list необходимо отправить в службу техподдержки для получения лицензионного файла.

Файл лицензии license.accordx можно положить в любое место в файловой системе (в примере из п.3.2.10 – в */etc/accordx/*), однако правильный путь необходимо прописать в initrd.

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. 3.2.10-3.2.11, и подсистема разграничения доступа к ресурсам ПЭВМ активизируется.

ВНИМАНИЕ!

Для корректной работы СПО «Аккорд-X K» в ОС RHEL 7.0 x64 требуется либо удалить пакеты fprintd и fprintd-pam, либо отключить их загрузку с помощью команды типа "systemctl mask fprintd.service" (предпочтителен первый вариант).

[7] Данная процедура выполняется в командной строке.

3.2.14 Перезагрузка ОС в мягком режиме работы СПО «Аккорд-X K»

На последней стадии установки и настройки СПО «Аккорд-X K» необходимо произвести перезагрузку ОС с установленным «мягким» режимом работы.

Мягкий режим устанавливается с помощью команды «Acx-admin config set 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 идентификаторам, 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 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-X» 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 («мягкий» режим таким образом будет автоматически отключен) и перезагрузиться.

ВНИМАНИЕ!

При отключении мягкого режима активизируются сразу две политики управления доступом, что может привести к невозможности загрузки ОС (из-за правил мандатной политики управления доступом).

3.2.15 Некоторые особенности настройки СПО «Аккорд-X K»

В процессе настройки СПО «Аккорд-X K» администратору БИ необходимо учитывать следующие особенности:

Для корректной работы некоторых компонентов «Аккорд-X K» (PAM, модули по работе с идентификаторами) при работающем SELinux необходимо отключить SELinux, *передав при загрузке в параметре ядра selinux=0 (см, например, рисунок 16).*

После активации подсистемы разграничения доступа и перезагрузки ОС в случае внесения каких-либо изменений в файл конфигурации или БД пользователей «Аккорд-X K» (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 «Аккорд-X K» будут активны БД и файл конфигурации, которые были актуальны на момент последней загрузки ОС.

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

В подсистеме контроля печати «Аккорд-X K» реализована возможность журналирования процедуры печати. Журнал находится в /var/log/accordx-print/acx-print.log. Одна запись журнала содержит следующие данные: дата и время, имя пользователя Linux, отправившего документ на печать, имя файла, отправленного на печать (но не полный путь к нему!), количество печатаемых копий, а также опции печати. Формат записи (строки) журнала имеет вид:

[<дата и время>]: User: '<имя пользователя>' | File: '<имя файла>' | Copies: '<количество копий>' | Options:

Примерный вид журнала представлен на рисунке 17.

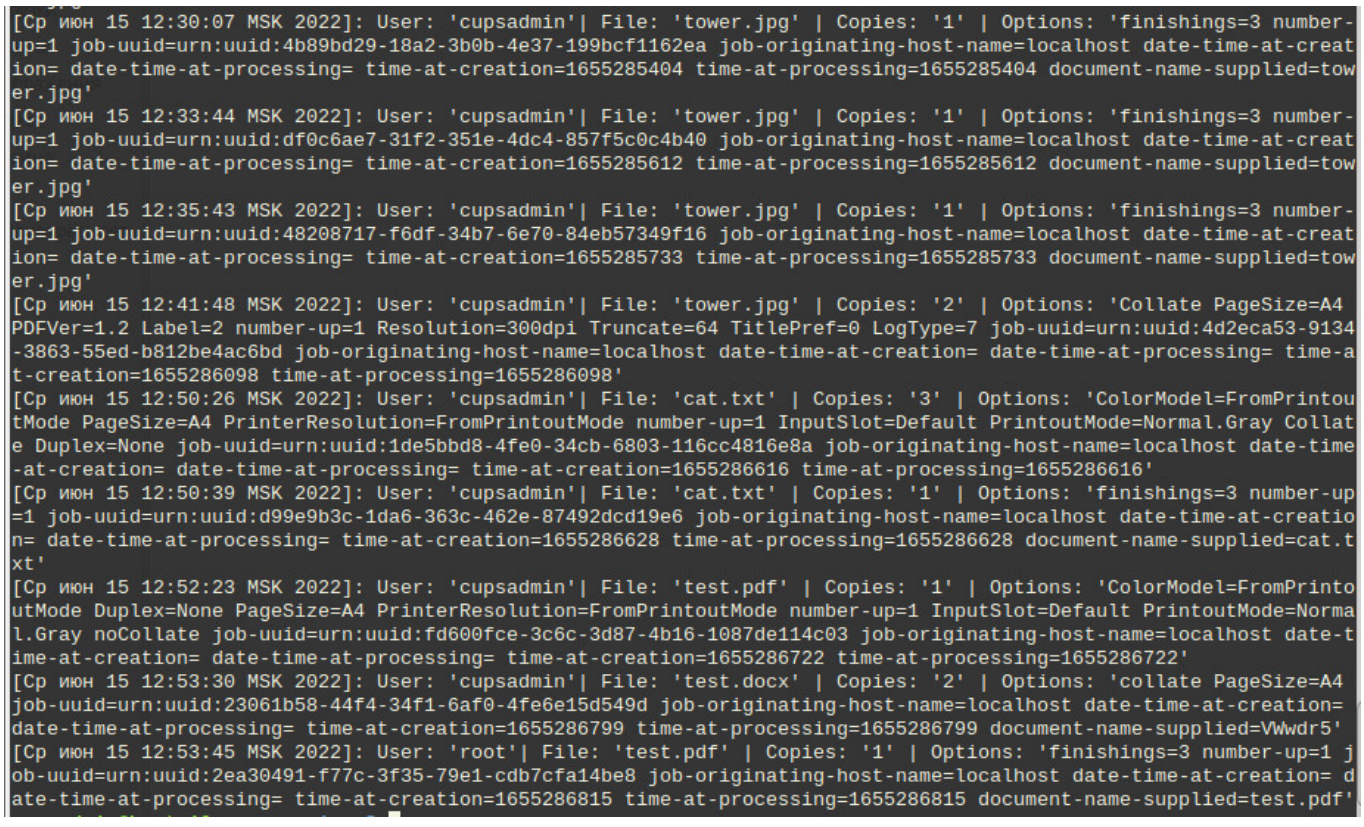

Рисунок 17 – Журнал контроля файлов, выводимых на печать

3.3.1 Установка модуля контроля печати

Модуль контроля печати поставляется в пакете acx-print.

Устанавливать acx-print необходимо командой (в зависимости от пакетного менеджера)

apt-get install ./acx-print*.deb

или

yum install -y ./acx-print*.rpm

3.3.2 Настройка ОС

Настройка ОС происходит при установке пакета acx-print.

В случае добавления новых принтеров необходимо обновить настройки, вызвав acx-print. Для отключения контроля печати следует использовать acx-print revert

4 ЭКСПЛУАТАЦИЯ СПО «АККОРД-X K»

4.1 Основные задачи, решаемые Администратором БИ при эксплуатации СПО «Аккорд-X K»

При эксплуатации СПО «Аккорд-X K» Администратор БИ решает следующие задачи:

- поддерживает средства защиты комплекса в работоспособном состоянии и контролирует правильность их работы;
- производит изменения в настройке средств защиты комплекса 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 комплекса;
- анализирует содержимое журнала регистрации событий, формируемого средствами комплекса, и на этой основе вырабатывает предложения по совершенствованию защитных механизмов, реализуемых средствами комплекса, принимает необходимые меры по совершенствованию системы защиты информации в целом.

ВНИМАНИЕ!
Непрерывная организационная поддержка функционирования средств защиты СПО предполагает обеспечение строгого соблюдения всеми пользователями требований СБИ (администратора БИ).

4.2 Вход в ОС в рамках действия СПО «Аккорд-X K»

При загрузке СВТ, защищенного СПО «Аккорд-X K», на начальном этапе загрузки ОС загружается СПО «Аккорд-X K» (из образа начальной загрузки initrd). При этом на экран выводится информация об успешном выполнении загрузки монитора разграничения доступа «Аккорд-X K», его конфигурации и БД (рисунок 18) (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).

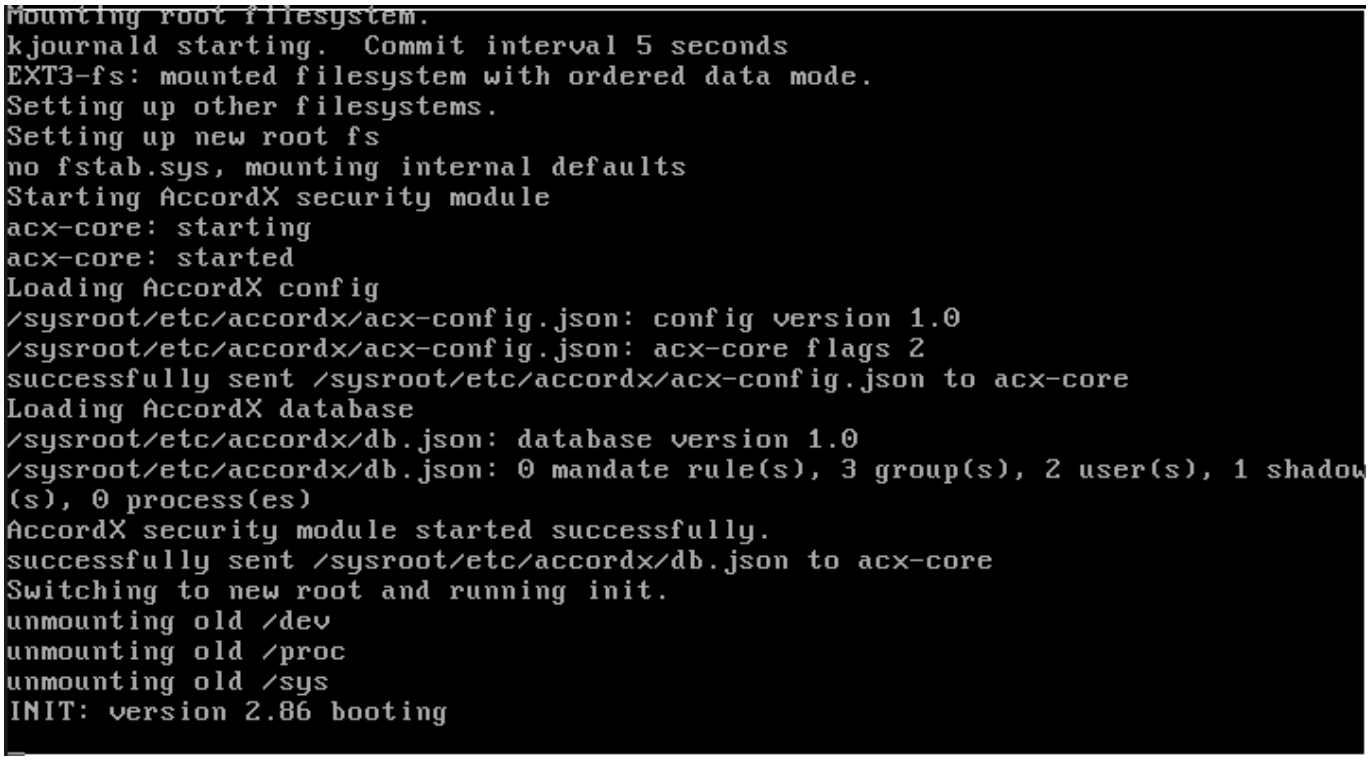

Рисунок 18 – Загрузка модуля разграничения доступа «Аккорд-X»

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 идентификатор (рисунок 19). Необходимо предъявить соответствующий идентификатор пользователя.

37222406.26.20.40.140.085 90

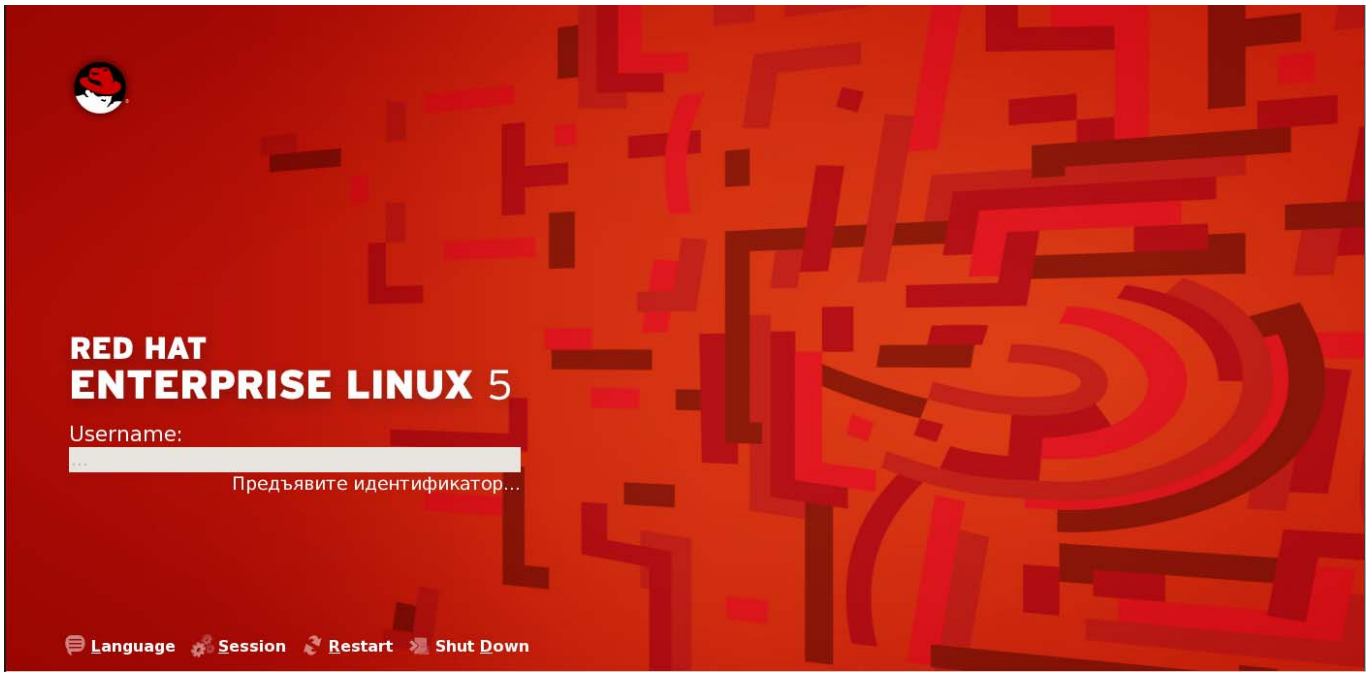

Рисунок 19 – Запрос идентификатора

После предъявления идентификатора в появившемся поле «Введите пароль» следует ввести соответствующий пароль пользователя, установленный для него в «Аккорд-Х К» (рисунок 20).

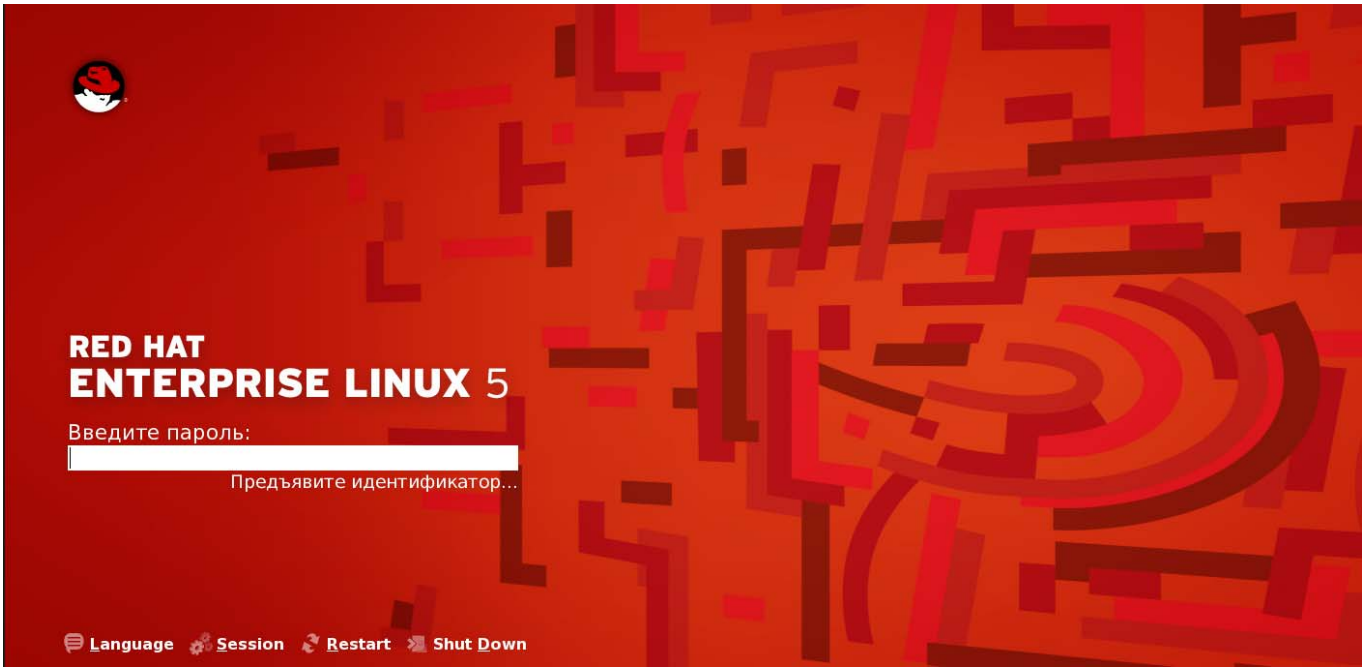

Рисунок 20 – Запрос пароля

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

ВНИМАНИЕ!

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

4.3 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):

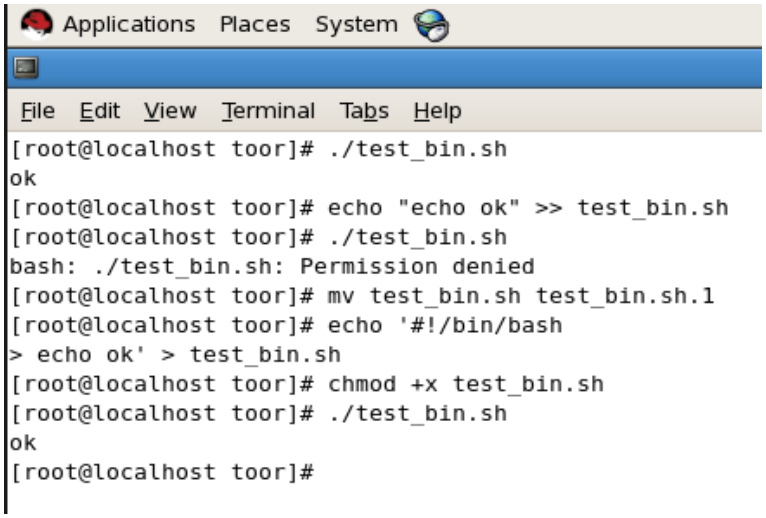

Рисунок 21 – Запрет запуска на выполнение файлов, целостность которых нарушена

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

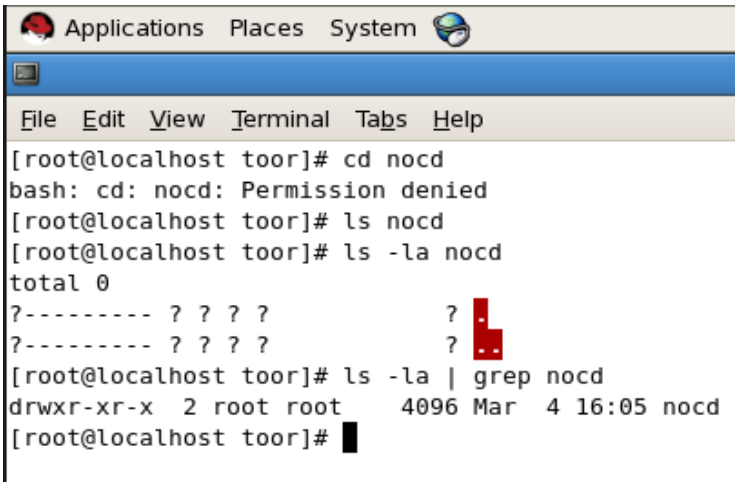

Рисунок 22 – Запрет перехода в каталог

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

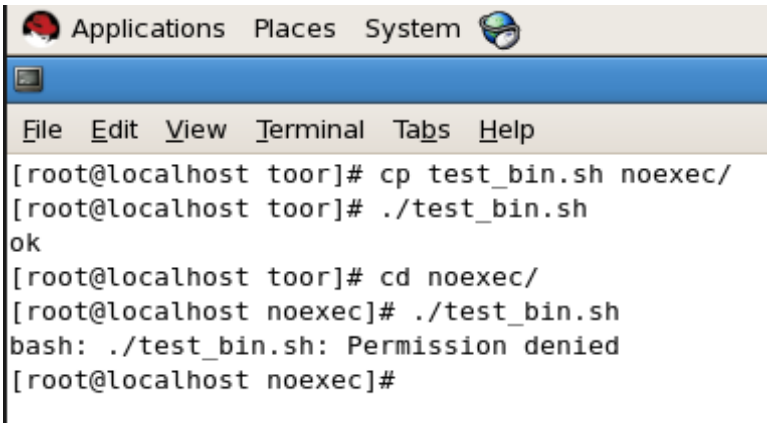

Рисунок 23 – Запрет запуска на выполнение программ

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

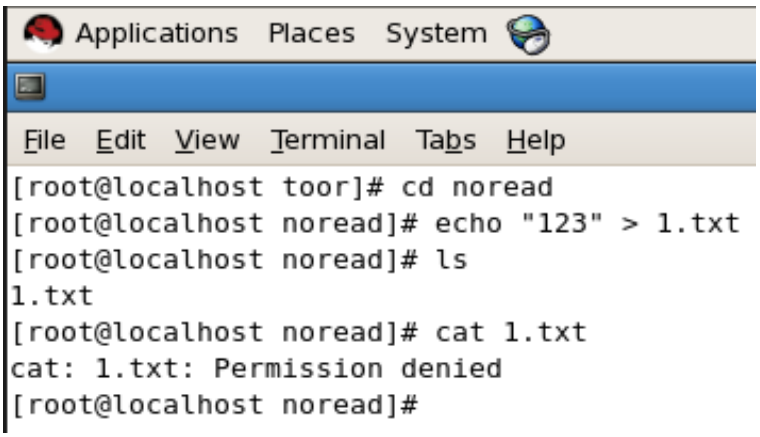

Рисунок 24 – Запрет открытия файлов на чтение

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).

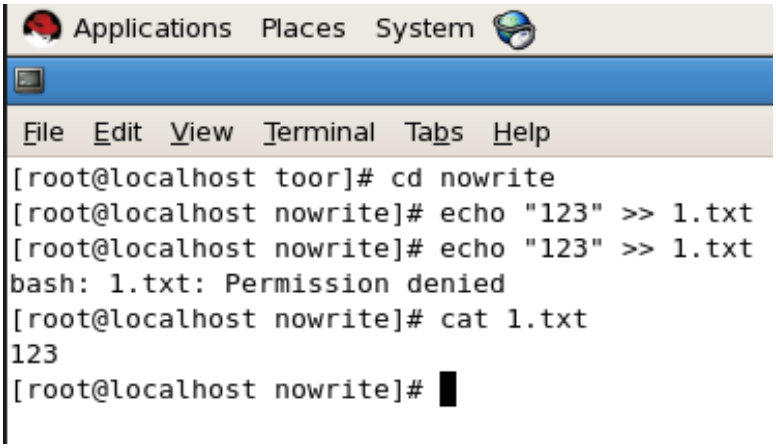

Рисунок 25 – Запрет на запись данных в объект

4.4 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:

- администратор БИ устанавливает уровень детальности журнала – низкая, средняя, высокая;
- для любого уровня детальности в журнале отражаются параметры регистрации и входа пользователя и попытки нарушения ПРД;
- для среднего уровня детальности в журнале отражаются дополнительно все попытки доступа к объектам по некоторым атрибутам доступа;
- для высокого уровня детальности в журнале отражаются дополнительно все попытки доступа к объектам (включая доступы на чтение, для которых в журнале будет создано большое количество событий).

Утилита администрирования комплекса **acx-admin log** предоставляет возможность просмотра, вывода на печать и архивации журнала регистрации событий.

Администратор БИ может просматривать журнал регистрации событий в «Аккорд-X K» (/var/log/accordx***, рисунок 26) 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 26 – 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 в формате POSIX time), например, 10:00:01[1390936318.188].

Для предоставления даты и времени в классическом формате можно, например, воспользоваться интерпретатором perl и выполнить:

acx-admin log show -m /var/log/accordx... | perl –pe 's/(\d+\t\d+:\d+:\d+\[)(\d+)(.\d+\])/localtime$2/e'

Так же можно выводить только события определенного типа, например, все события входа пользователей, нарушений динамического контроля целостности и дискреционных правил доступа:

acx-admin log show -m /var/log/accordx... | perl -pe 's/(\d+\t\d+:\d+:\d+\[)(\d+)(.\d+\])/localtime$2/e' | grep -e login -e int -e discr

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.

5 РАБОТА СПО ЧЕРЕЗ ПОЛЬЗОВАТЕЛЬСКОЕ GUI-ПРИЛОЖЕНИЕ ИЛИ WEB-ПРИЛОЖЕНИЕ

5.1 Настройка работы через графический интерфейс

Для работы с «Аккорд-X K» **через пользовательское GUI-приложение** следует вызвать из консоли утилиту acx-gui-qt (от имени пользователя root).

Чтобы настроить работу с «Аккорд-X K» **через Web-приложение**, следует запустить от имени root сервис (демон) по пути /root/acx-gui-web/acx-gui-daemon (для запуска в фоновом режиме – например, "/root/acx-gui-web/acx-gui-daemon&"), затем запустить из любого браузера с поддержкой websockets само Web-приложение из файла /root/acx-gui-web/index.html.

В Н И М А Н И Е !

На данный момент GUI и Web-приложения «Аккорд-X K» находятся в стадии бета-тестирования, в связи с чем их работоспособность не гарантируется для всех поддерживаемых ОС. При этом работоспособность консольных утилит гарантируется для всех ОС.

5.2 Начальная конфигурация

После выполнения процесса установки ПО разграничения доступа необходимо провести начальную конфигурацию.

Для этого следует в главном окне программы управления выбрать вкладку «Конфигурация» (рисунок 27, рисунок 28) и нажать кнопку <Создать>.

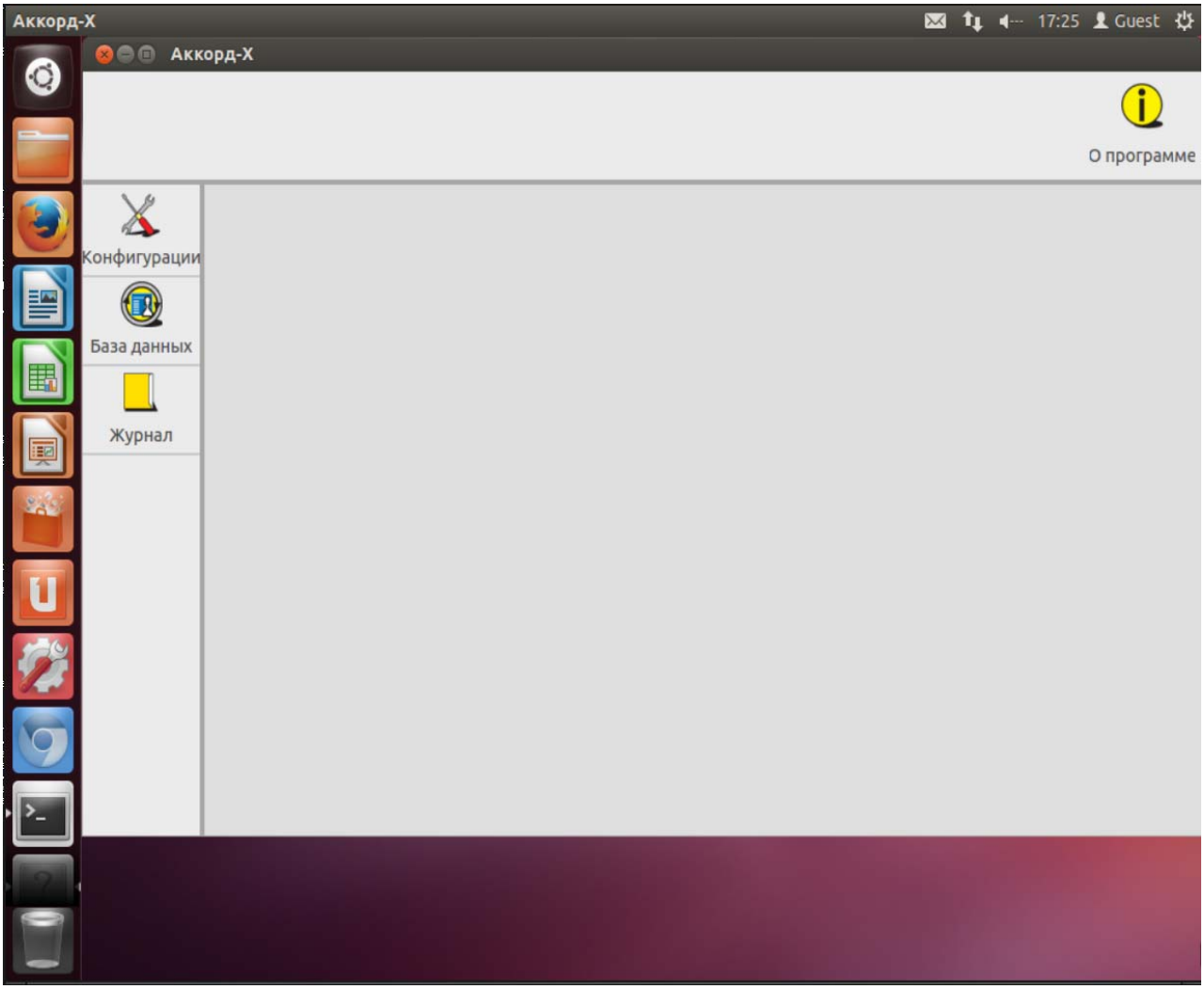

Рисунок 27 - Главное окно утилиты управления комплексом (пользовательское GUI-приложение)

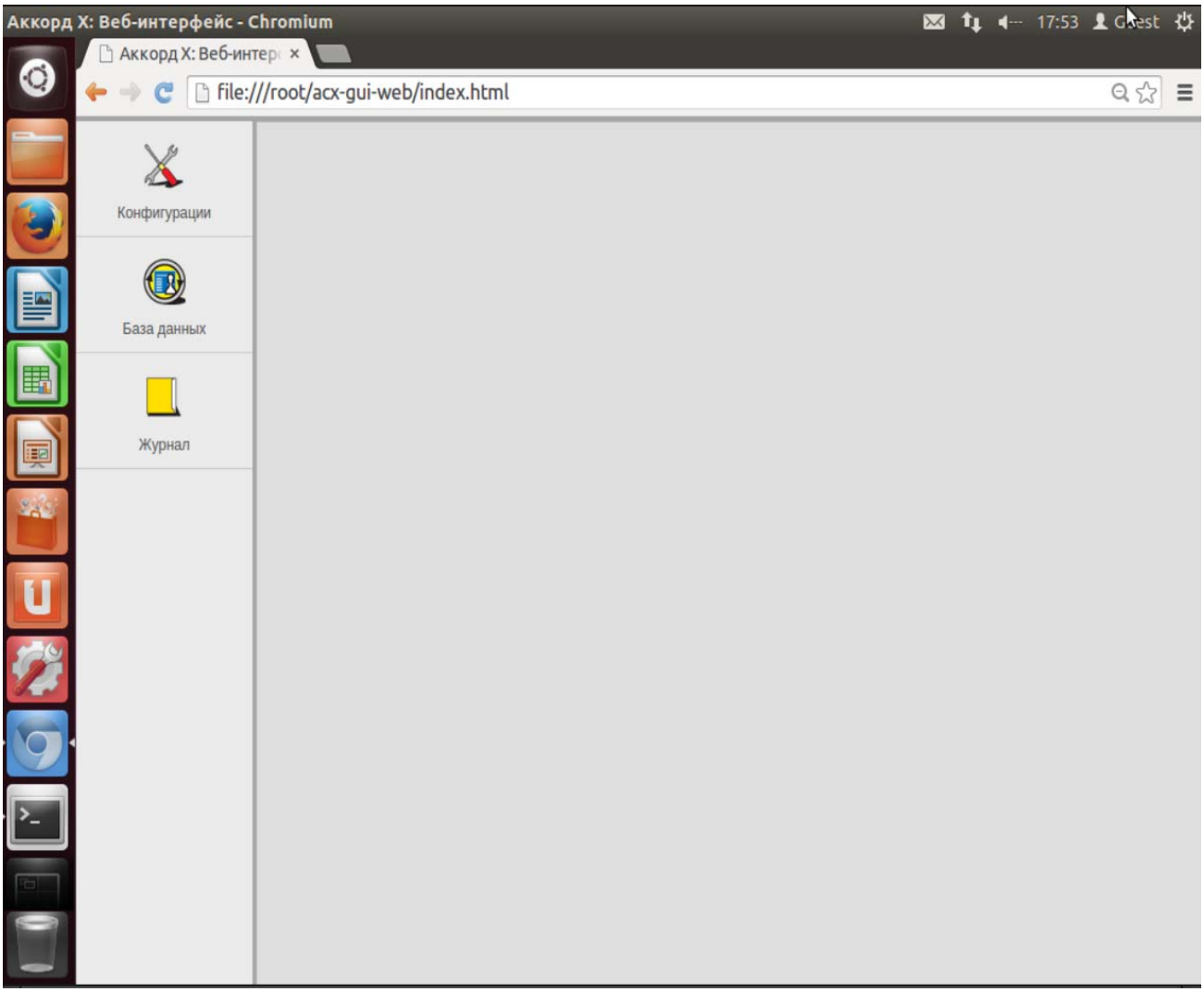

Рисунок 28 - Главное окно утилиты управления комплексом (Web-приложение)

В появившемся далее окне (рисунок 29, рисунок 30) следует указать путь к расположению создаваемого файла конфигураций.

Установка флага «По умолчанию» влечет сохранение файла конфигураций в каталог по умолчанию (/etc/accordx/acx-config.json). При необходимости можно сменить каталог посредством ручного редактирования или с помощью стандартного диалога, вызываемого нажатием кнопки <...>. Если указанный каталог не существует, он будет создан автоматически.

В случае установки флага «С конфигурациями по умолчанию» файл создается с конфигурациями, выставленными по умолчанию.

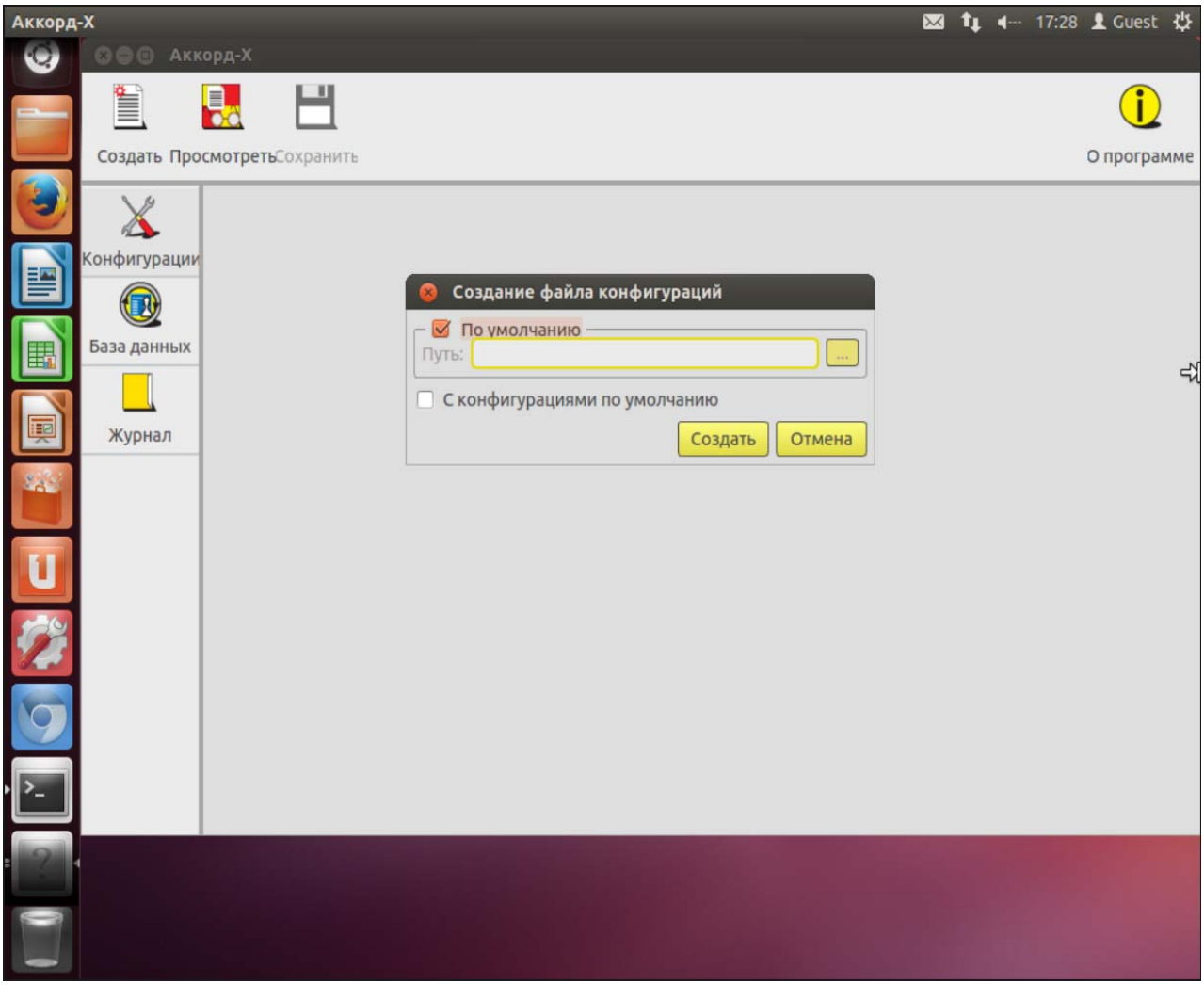

Рисунок 29 - Создание файла конфигураций (пользовательское GUI-приложение)

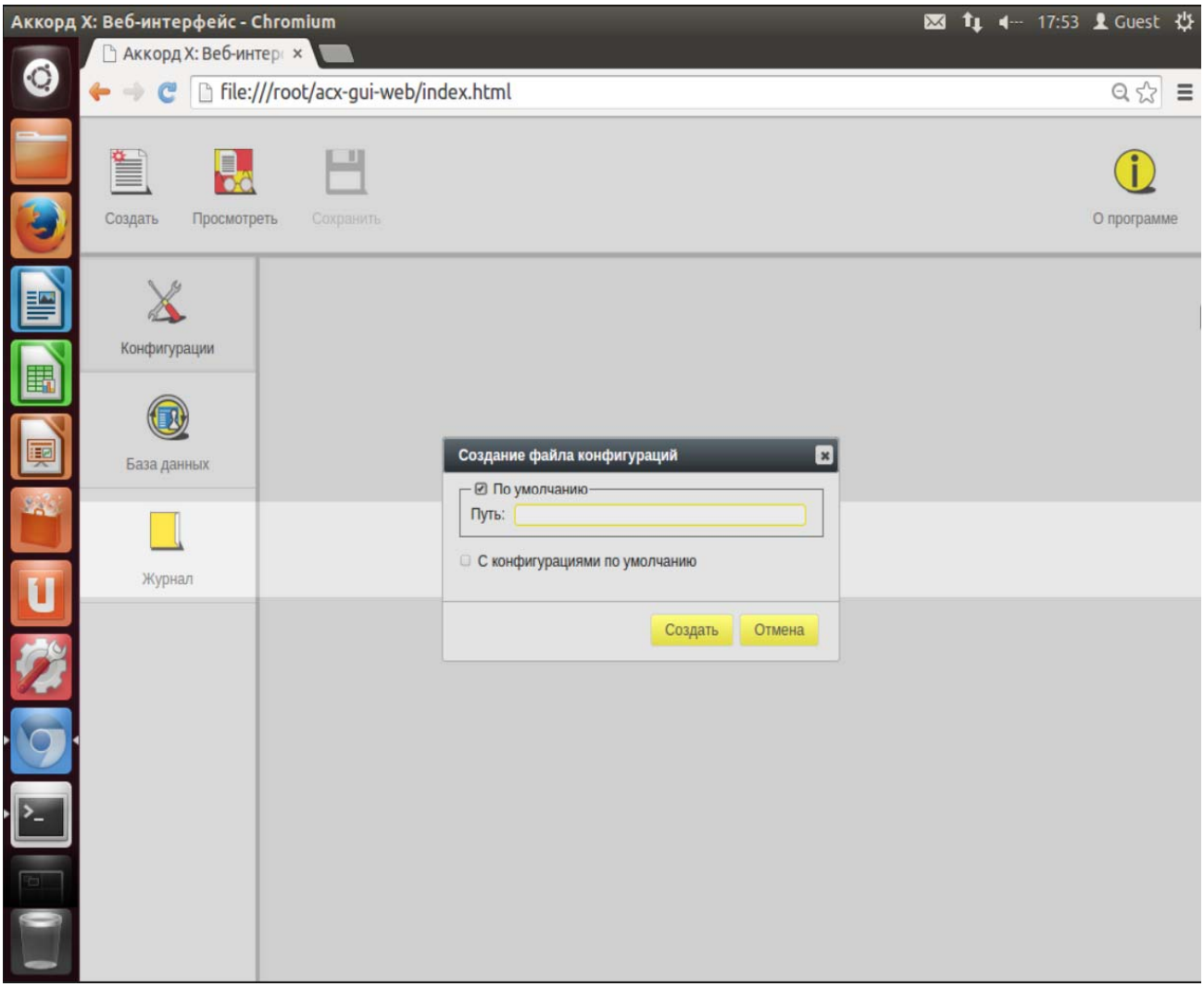

Рисунок 30 - Создание файла конфигураций (пользовательское Web-приложение)

По нажатии кнопки <Создать> на экран выводится список конфигураций (рисунок 31, рисунок 32). Настройка конфигураций выполняется посредством установки соответствующих флагов и заполнения соответствующих полей.

Для просмотра и редактирования доступны следующие параметры конфигурации:

1. Общие:
   - «Путь к БД» – путь к файлу с базой данных;
   - «Путь к журналу» – путь к файлу с журналом.
2. Организация:
   - «Название» – название организации;
   - «Телефон» – контактный телефон организации.
3. Флаги ядра – используется для выполнения настроек ядра защиты комплекса. Параметры блока:
   - «Включить ПРД» – включение разрешительных политик разграничения доступа;

- «Включить дискреционные ПРД» – включение дискреционной политики разграничения доступа;
- «Включить мандатные ПРД» – включение политики разграничения доступа на основе иерархических меток;
- «Включить Star-property-свойство (запрет записи «вниз»)» – включение правила запрета записи «вниз» в политике разграничения доступа на основе иерархических меток;
- «Включить мягкий режим» – включение мягкого режима;
- «Включить управление точками монтирования ФС» – включения контроля точек монтирования;
- «Включить динамический СКЦ» – включение динамического контроля целостности;
- «Включить контроль печати» – включение контроля печати;
- «Включить подсистему очистки памяти» – включение очистки оперативной памяти;
- «Уровень журнала по умолчанию» – уровень детальности журнала событий.

4. «Расшифровка уровней доступа» – используется для задания соответствия между строками и иерархическими метками.

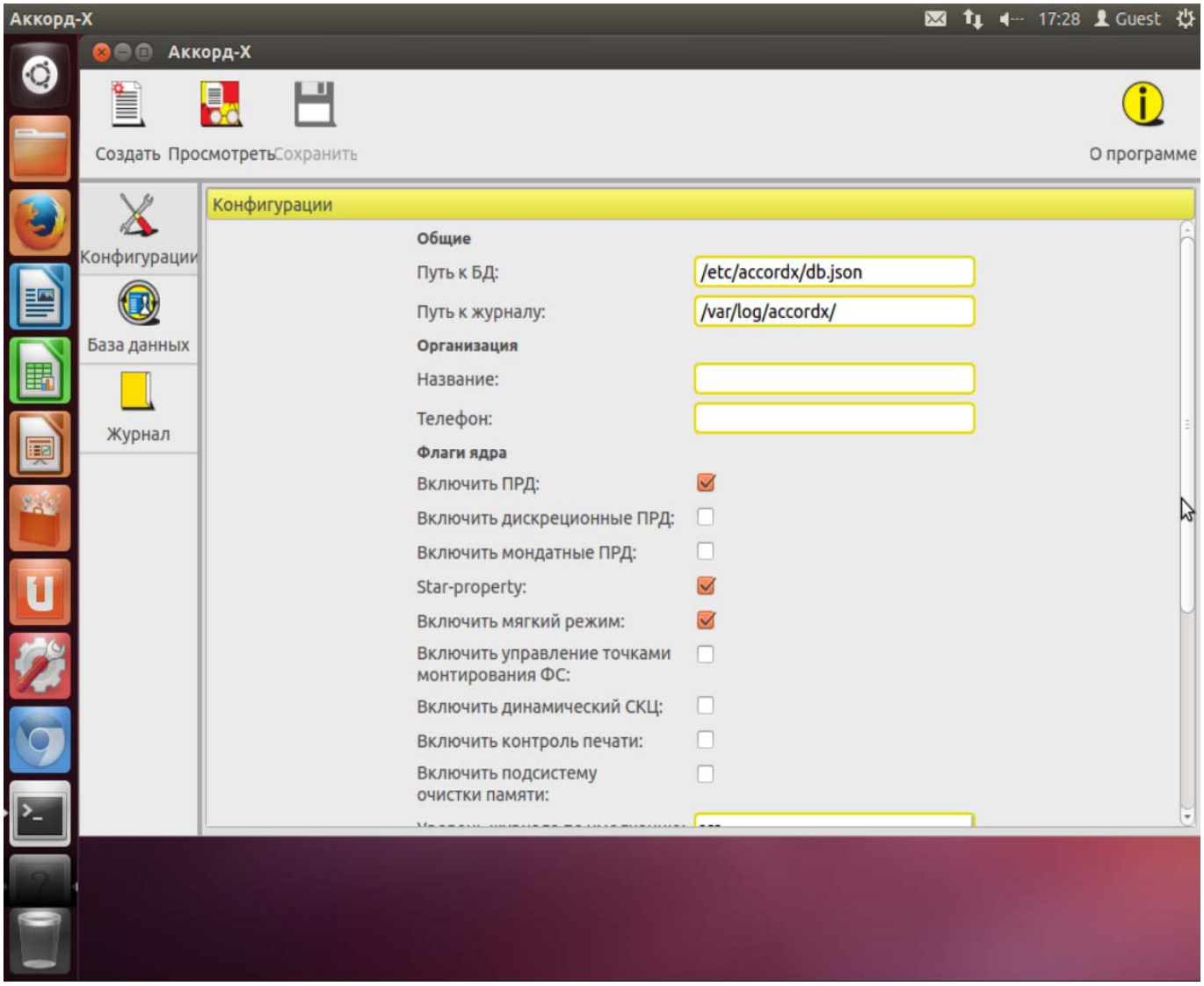

Рисунок 31 - Настройка конфигураций (пользовательское GUI-приложение)

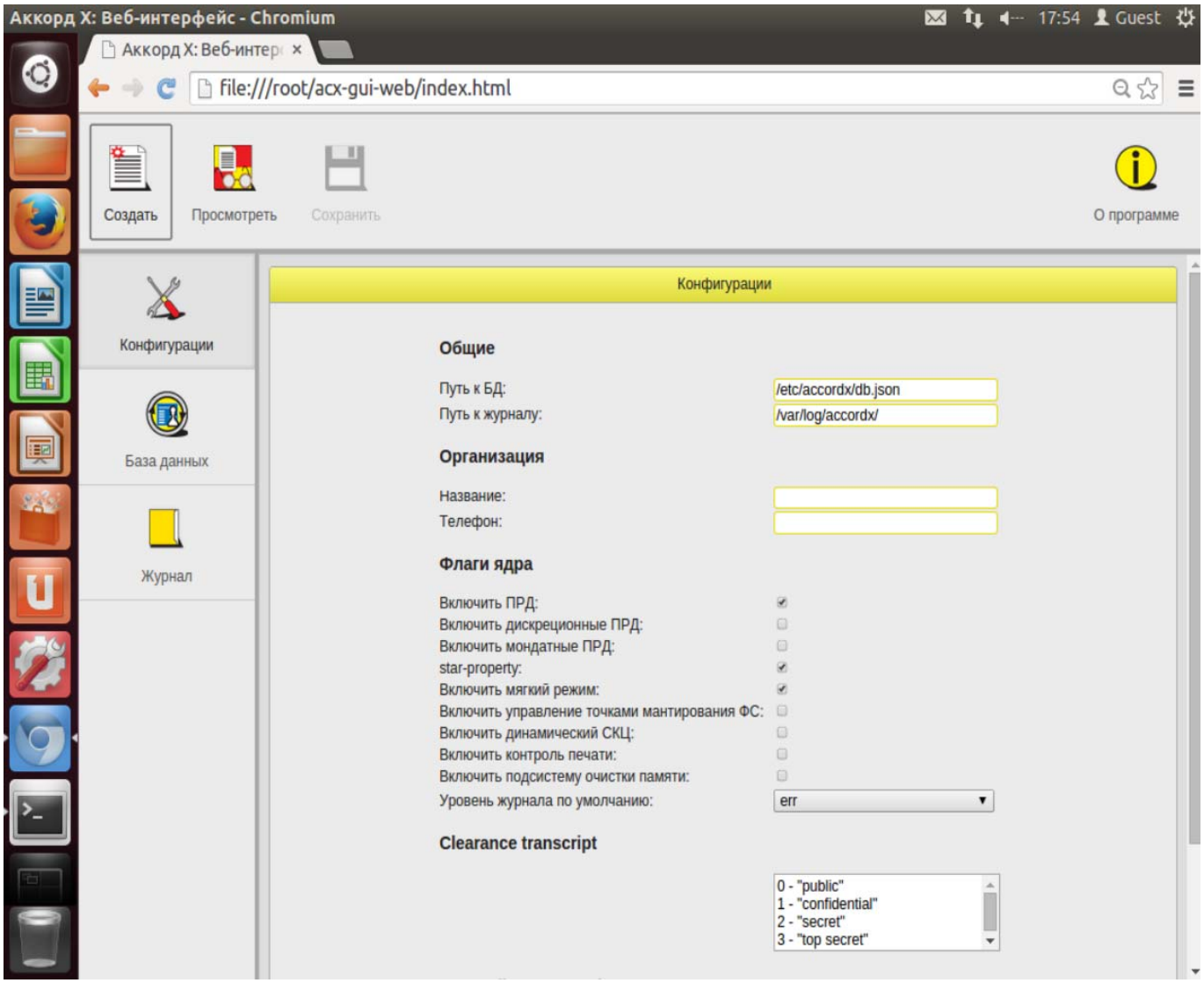

Рисунок 32 - Настройка конфигураций (Web-приложение)

Просмотр и редактирование содержимого файла конфигураций (уже существующего) осуществляется с помощью кнопки <Просмотреть> на вкладке «Конфигурации» главного окна программы администрирования (при нажатии кнопки <Просмотреть> на экран выводится окно выбора файла конфигураций).

5.3 Создание базы данных пользователей

Для создания базы данных пользователей следует в главном окне программы администрирования перейти на вкладку «База данных» и нажать кнопку <Создать>.

В появившемся далее окне следует указать путь к расположению создаваемого файла с базой данных (рисунок 33, рисунок 34).

Установка флага «По умолчанию» влечет сохранение файла с базой данных в каталог по умолчанию (/etc/accordx/db.json). При необходимости можно сменить каталог посредством ручного редактирования или с помощью

стандартного диалога, вызываемого нажатием кнопки <...>. Если указанный каталог не существует, он будет создан автоматически.

В случае установки флага «С параметрами по умолчанию» файл создается с параметрами БД, выставленными по умолчанию.

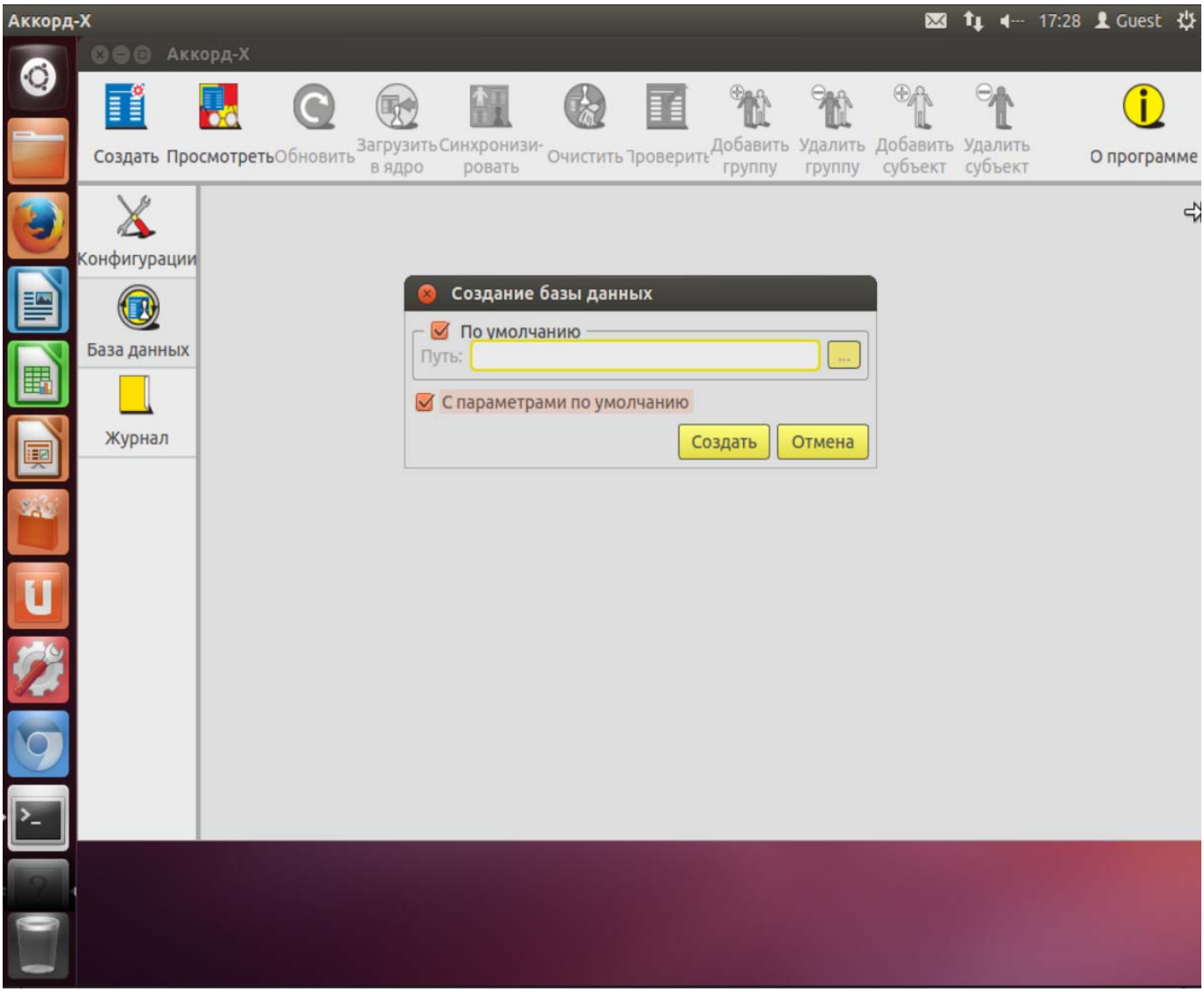

Рисунок 33 - Создание базы данных (пользовательское GUI-приложение)

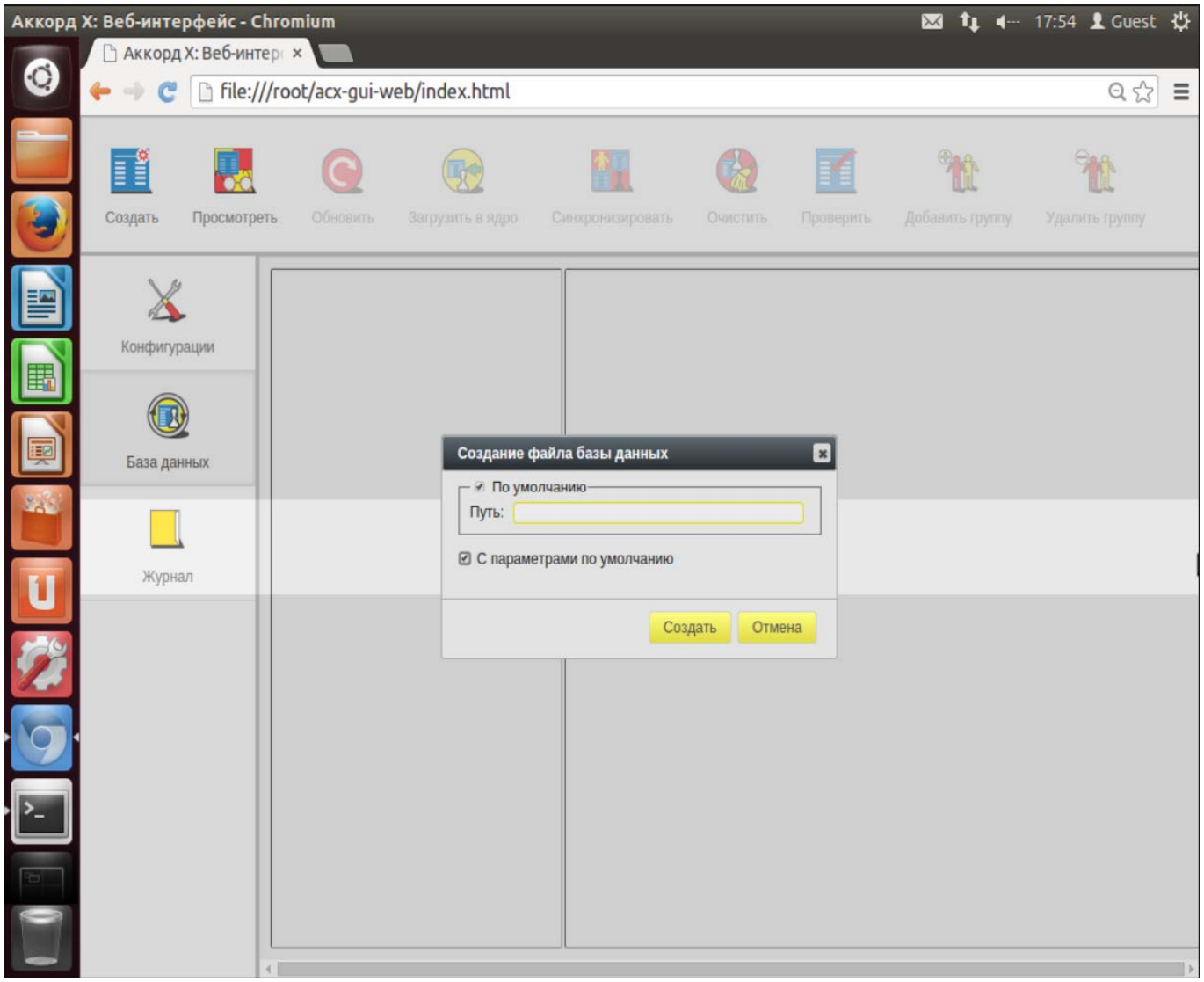

Рисунок 34 - Создание базы данных (Web-приложение)

После создания файла с базой данных на вкладке «База данных» главного окна программы управления отображается структура созданной БД (рисунок 35).

В случае если в процессе создания БД установлен флаг:

- «По умолчанию», на вкладке «База данных» путь к расположению файла с БД отображается как «По умолчанию»;
- «С параметрами по умолчанию», на вкладке «База данных» отображается структура БД со стандартными учетными записями.

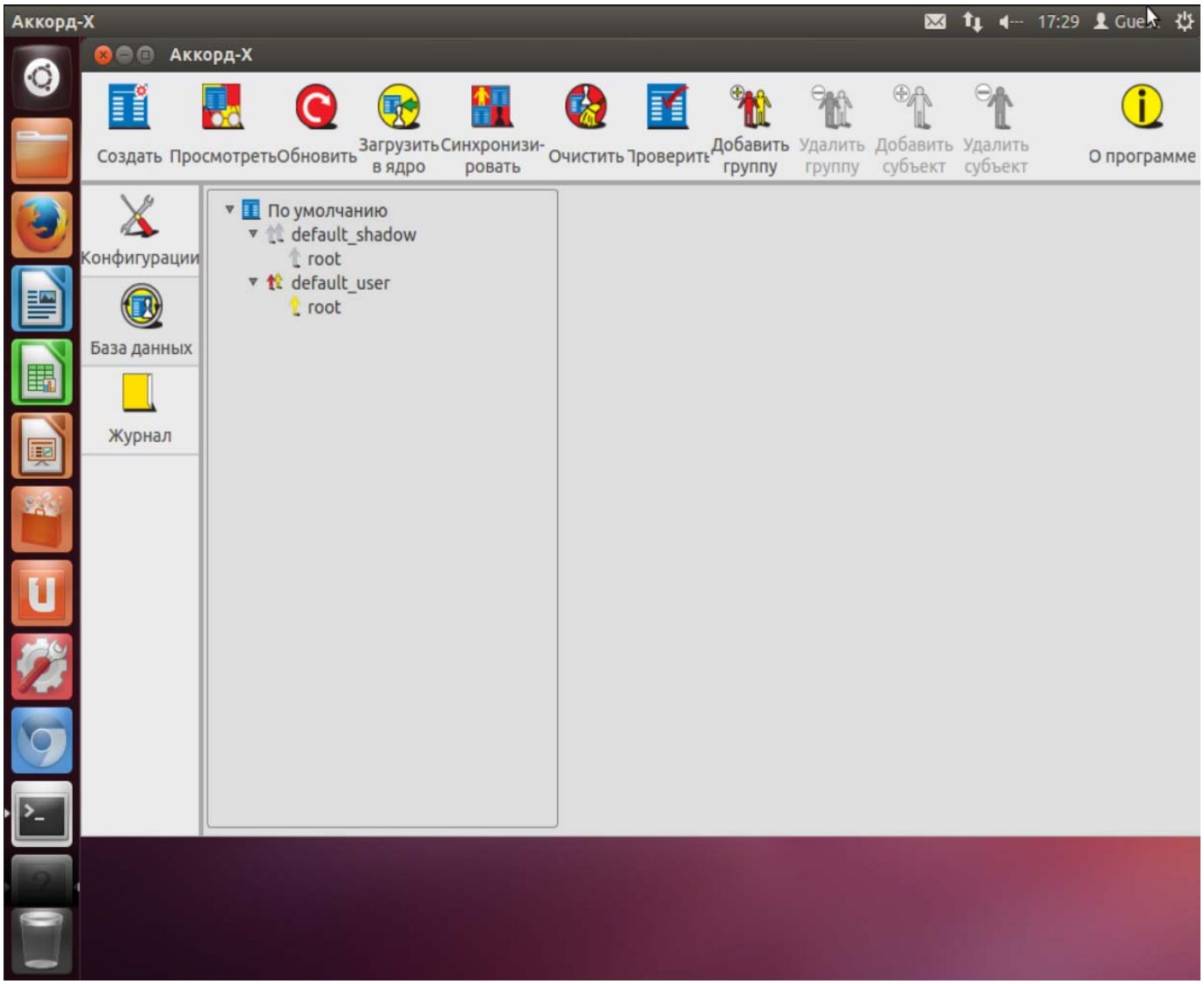

Рисунок 35 - База данных со стандартными пользователями (пользовательское GUI-приложение)

В Н И М А Н И Е !

Чтобы в процессе дальнейшего функционирования «Аккорд-X К» можно было выполнить вход в ОС в качестве Администратора БИ (суперпользователя; пользователя root), после создания базы данных пользователей для него необходимо назначить идентификатор и задать пароль в БД (данную процедуру необходимо выполнить потому, что при создании БД использовалась опция автосоздания нужных по умолчанию пользователей, и, следовательно, идентификатор и пароль для пользователя root еще не заданы).

При этом необходимо удостовериться, что uid и пароль этого пользователя совпадает со значениями из файла /etc/passwd.

По завершении процедуры создания БД и появления структуры БД на вкладке «База данных» на экран автоматически выводится окно с предложением установить идентификатор и задать пароль пользователю root. Необходимо нажать кнопку <Да> (рисунок 36).

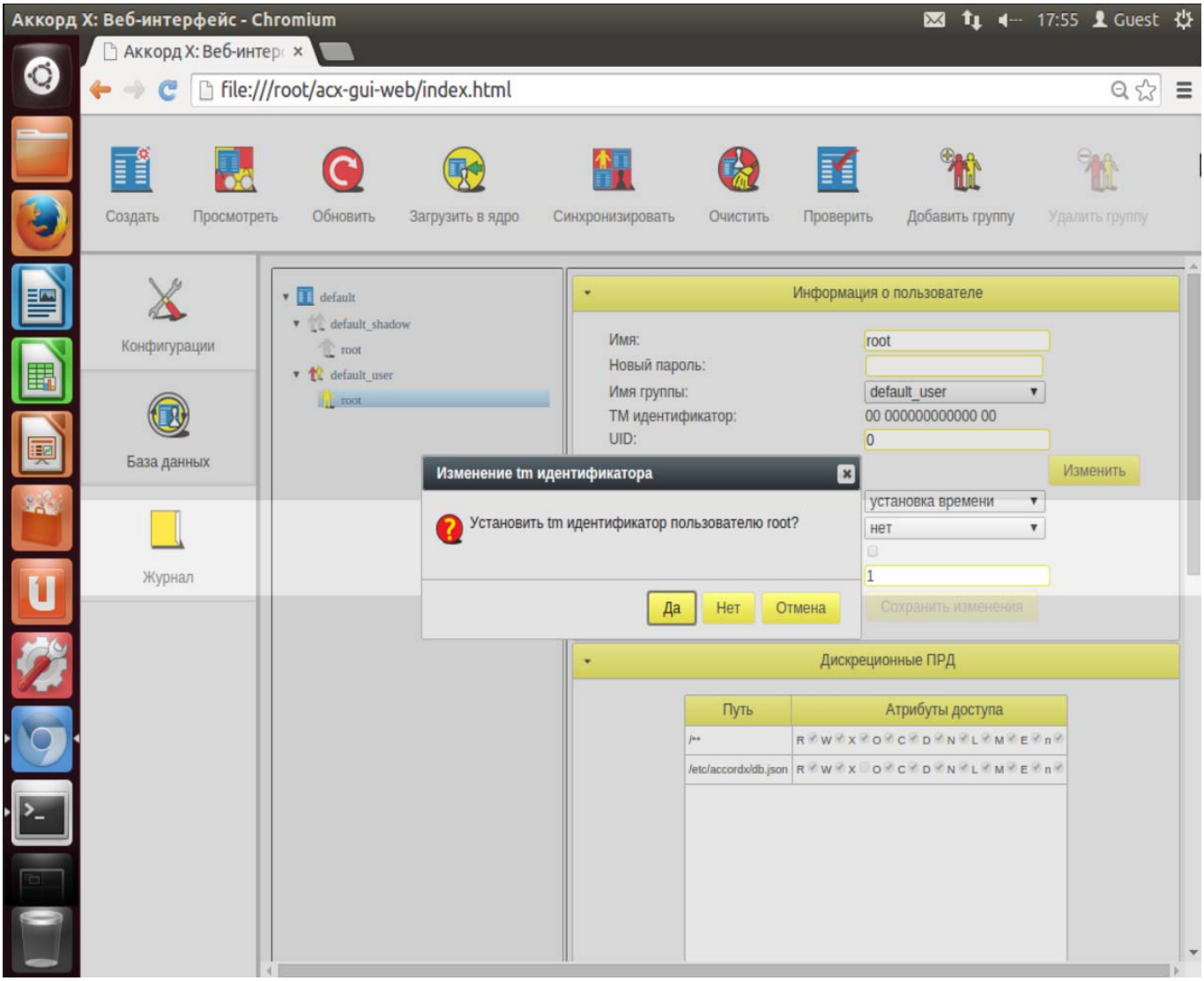

Рисунок 36 - Запрос на установку идентификатора для пользователя root (Web-приложение)

В появившемся далее окне следует задать новый пароль для учетной записи пользователя root, предъявить идентификатор и нажать кнопку <Редактировать> (рисунок 37, рисунок 38).

37222406.26.20.40.140.085 90

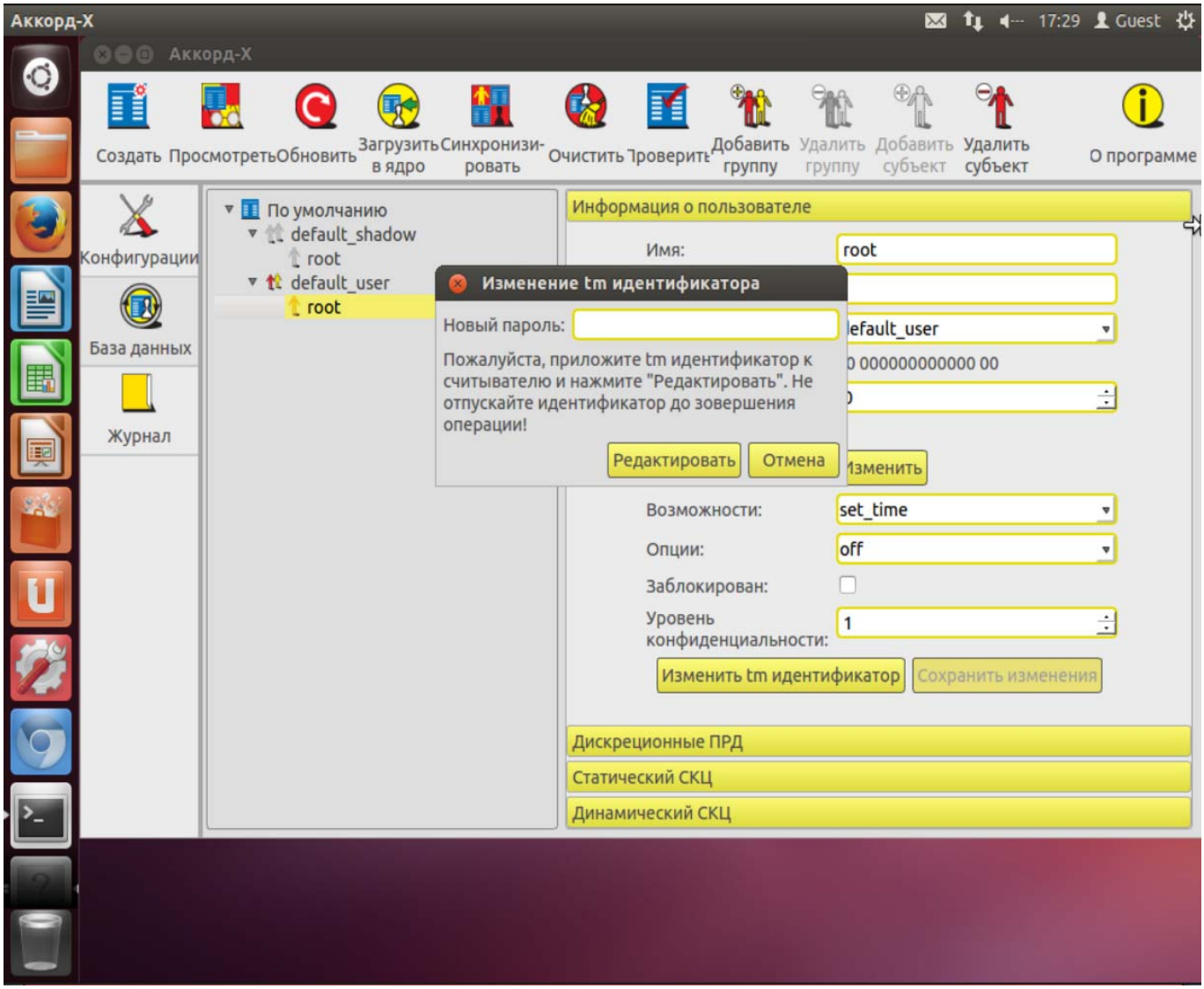

Рисунок 37 - Установка пароля и ТМ-идентификатора пользователю root (пользовательское GUI-приложение)

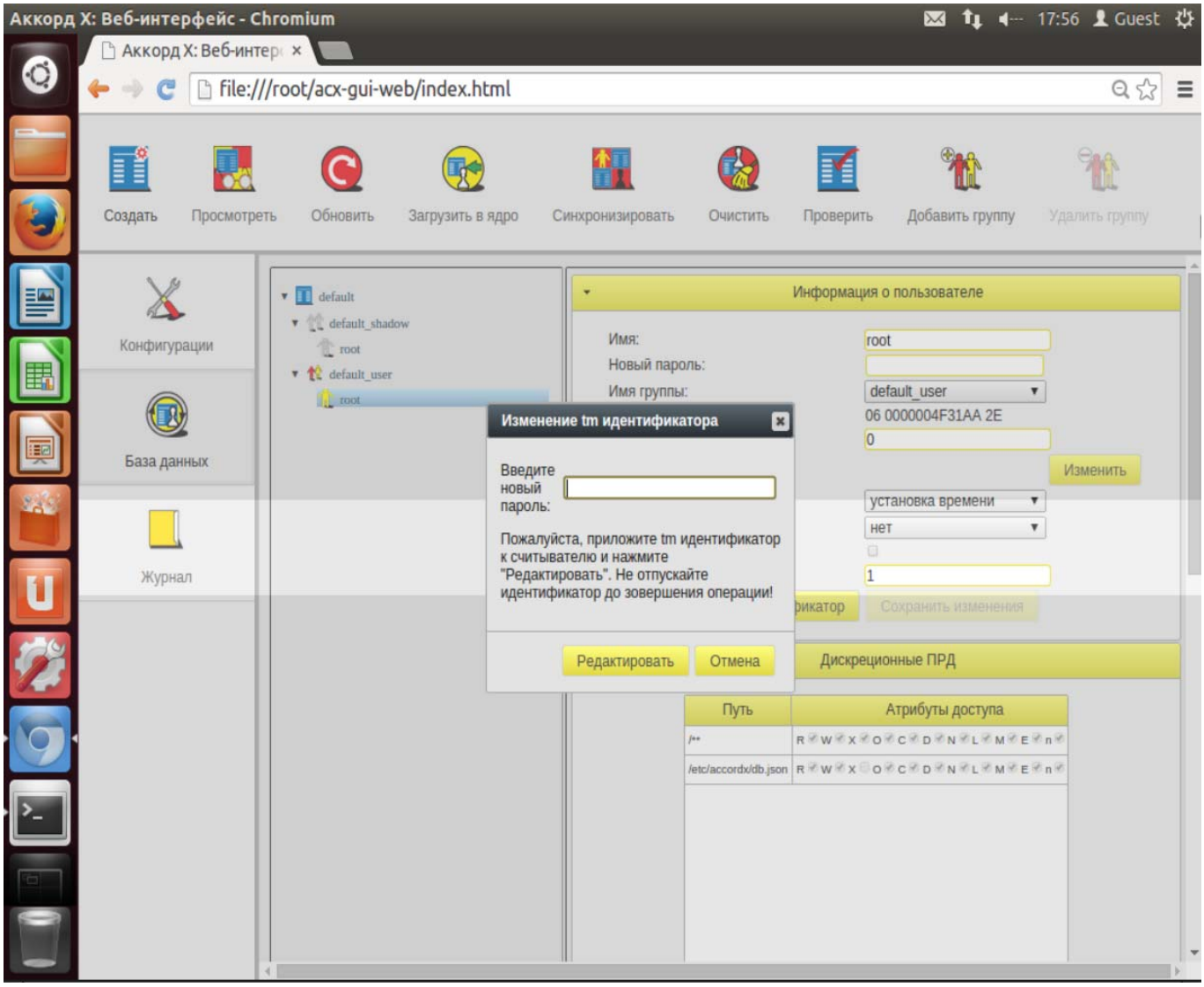

Рисунок 38 - Установка пароля и ТМ-идентификатора пользователю root (Web-приложение)

5.4 Создание групп пользователей

Для создания группы пользователей следует на вкладке «База данных» нажать кнопку <Добавить группу>.

В появившемся далее окне следует выбрать тип создаваемой группы и нажать кнопку <Добавить>.

На данный момент группирование пользователей не оказывает влияния на общую работу комплекса – группы используются для удобства. Однако необходимо учитывать, что для корректной работы комплекса должны выполняться условия, описанные в настоящем пункте (см. описание варианта для работы в командной строке).

37222406.26.20.40.140.085 90

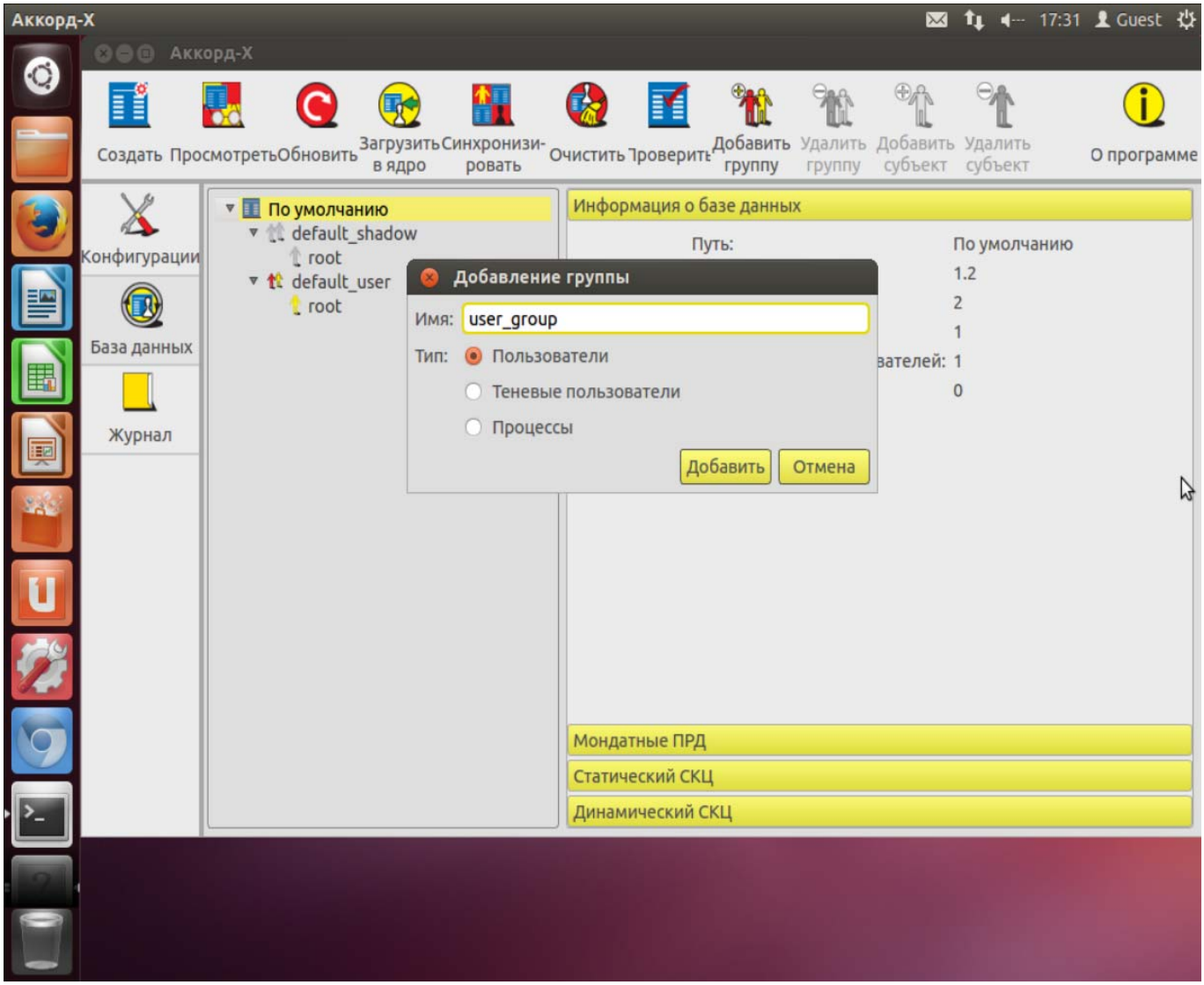

Рисунок 39 - Создание группы пользователей (пользовательское GUI-приложение)

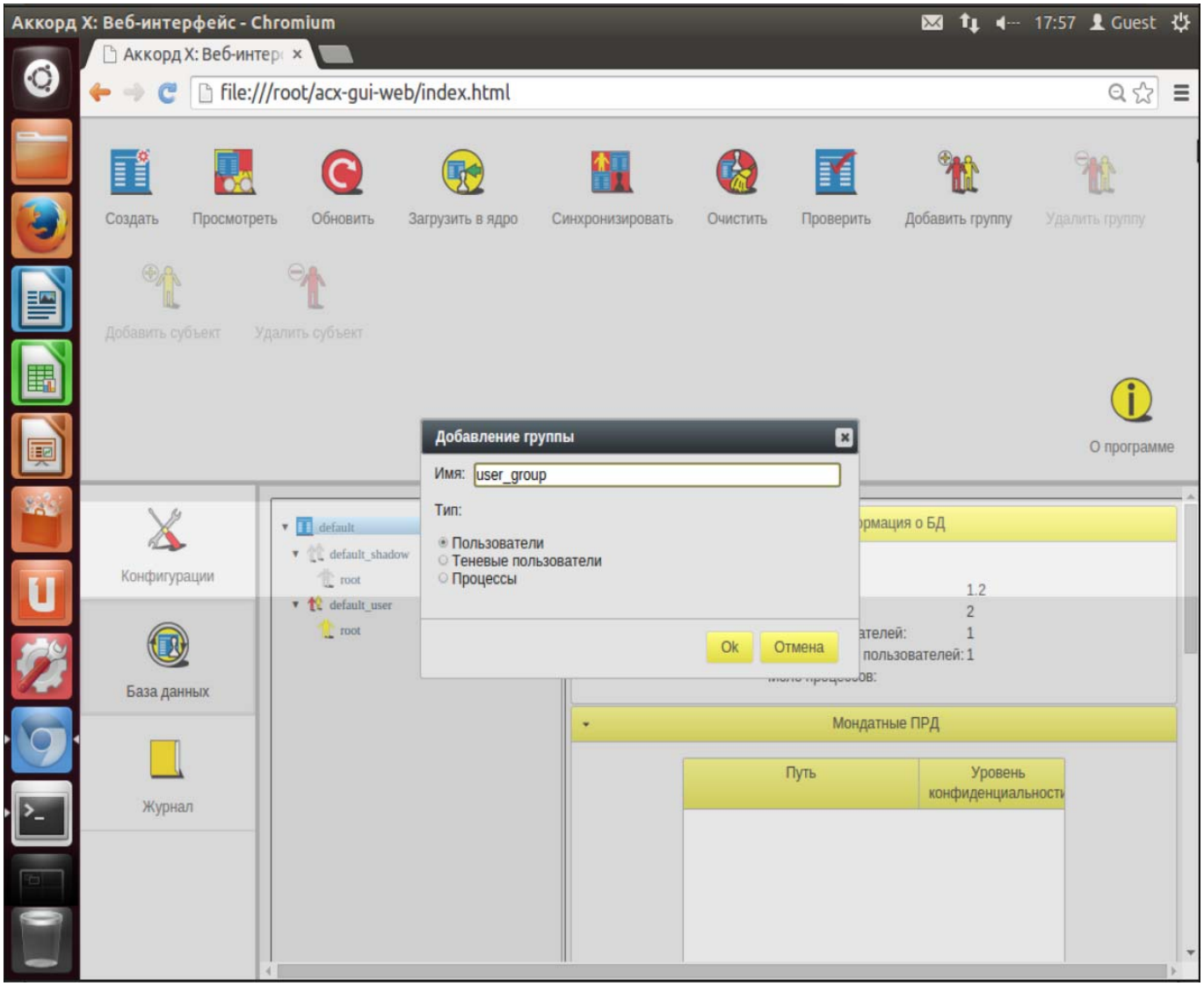

Рисунок 40 - Создание группы пользователей (Web-приложение)

5.5 Создание учетных записей пользователей

Для создания нового пользователя следует на вкладке «База данных» нажать кнопку <Добавить пользователя>.

В появившемся далее окне следует задать необходимые параметры учетной записи создаваемого пользователя и нажать кнопку <Добавить> (рисунок 41, рисунок 42).

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 дискреционные ПРД и ПРД на основе иерархических меток.

37222406.26.20.40.140.085 90

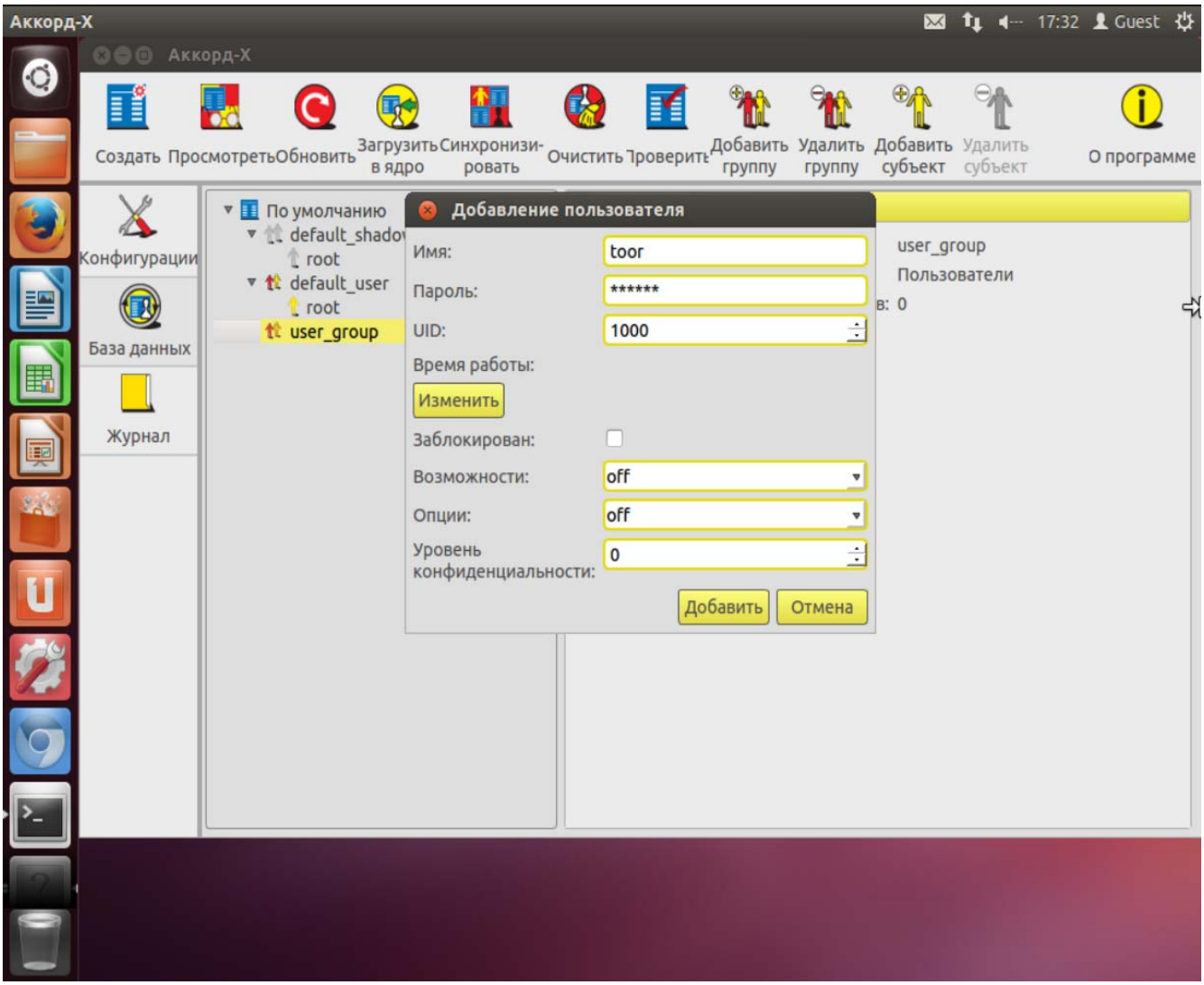

Рисунок 41 - Добавление пользователя (пользовательское GUI-приложение)

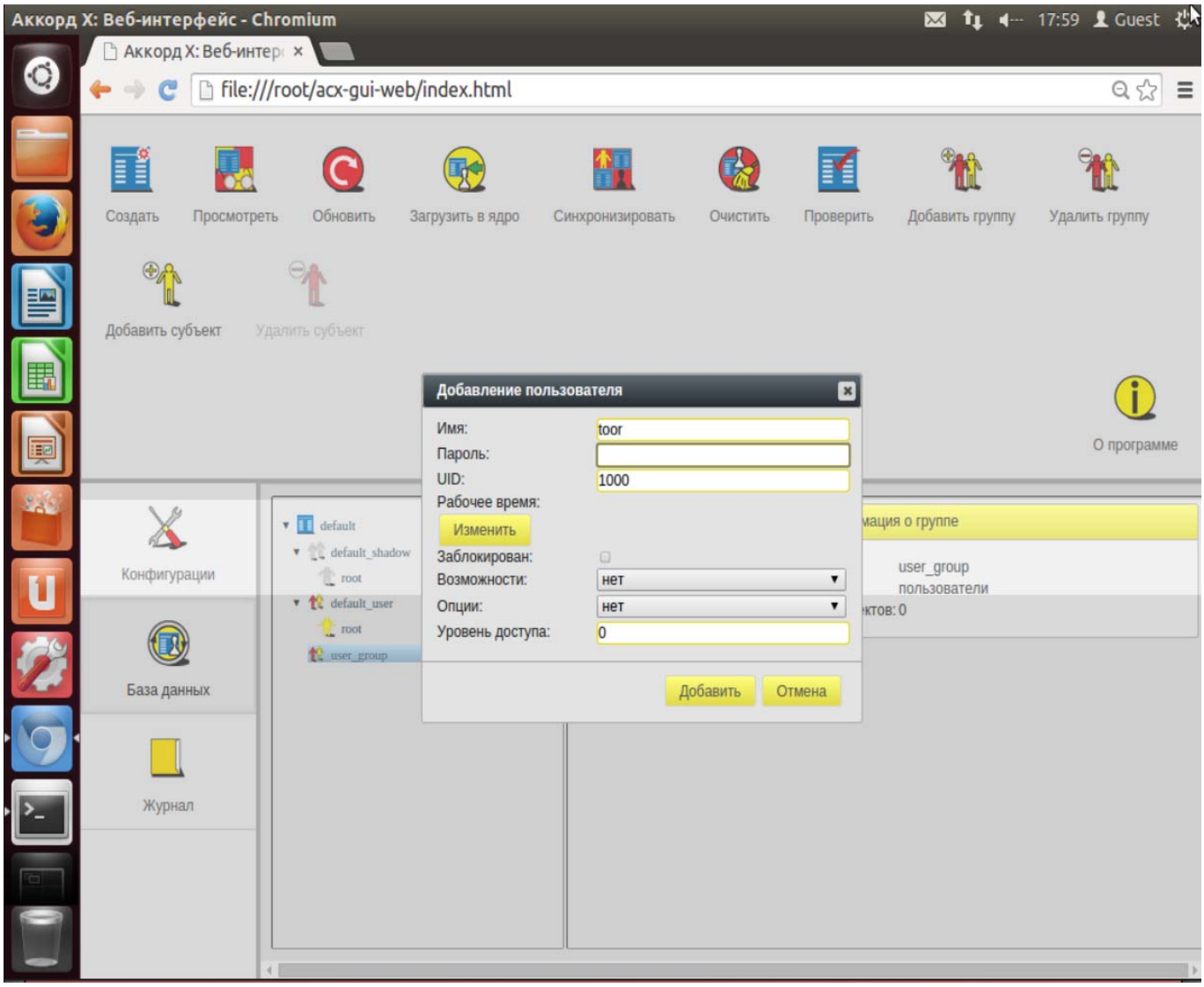

Рисунок 42 - Добавление пользователя (Web-приложение)

После выполнения описанной последовательности действий пользователь с именем toor появляется в базе данных пользователей «Аккорд-X K» (рисунок 43, рисунок **44**).

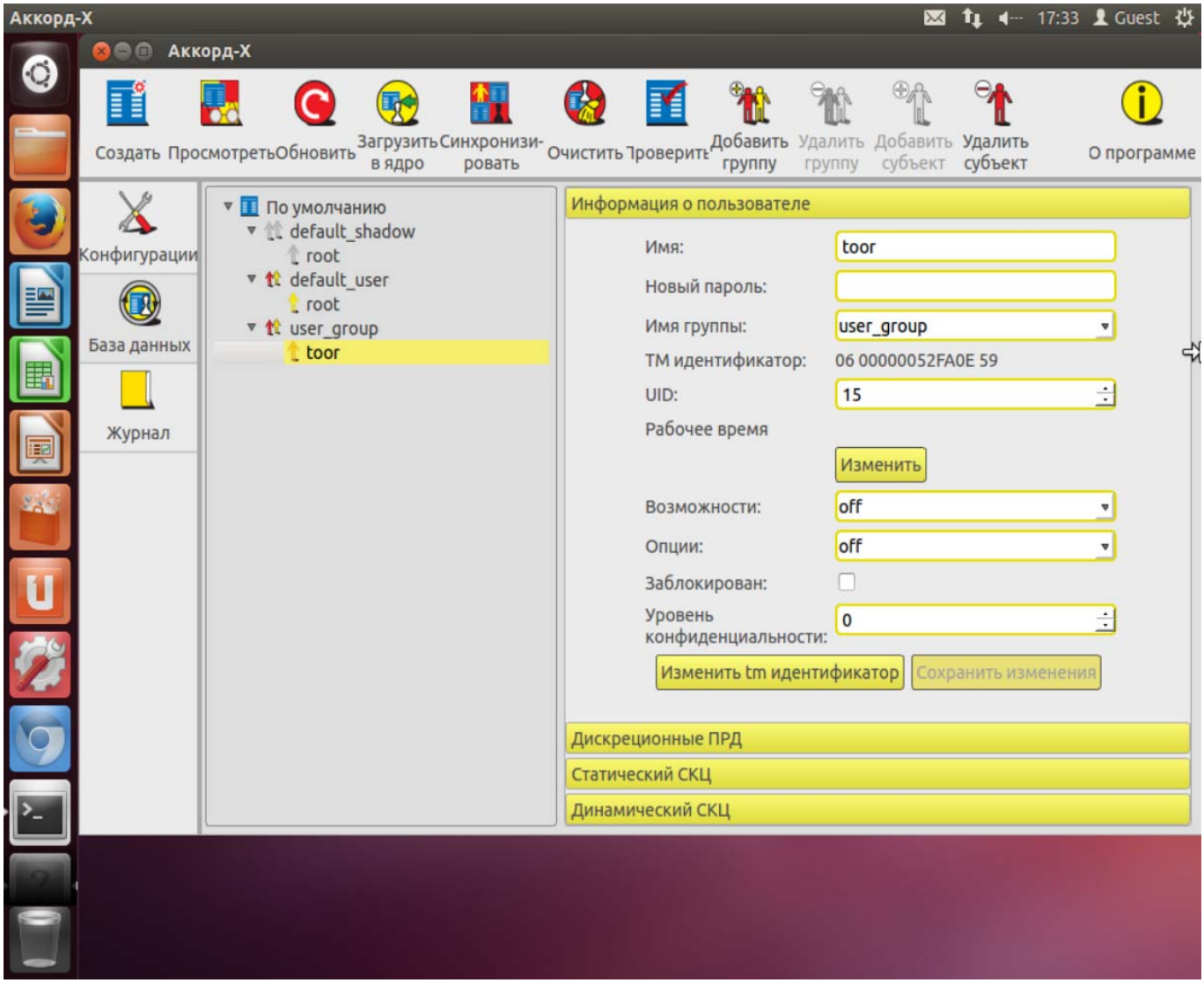

Рисунок 43 - Пользователь с именем toor в базе данных пользователей «Аккорд-X К» (пользовательское GUI-приложение)

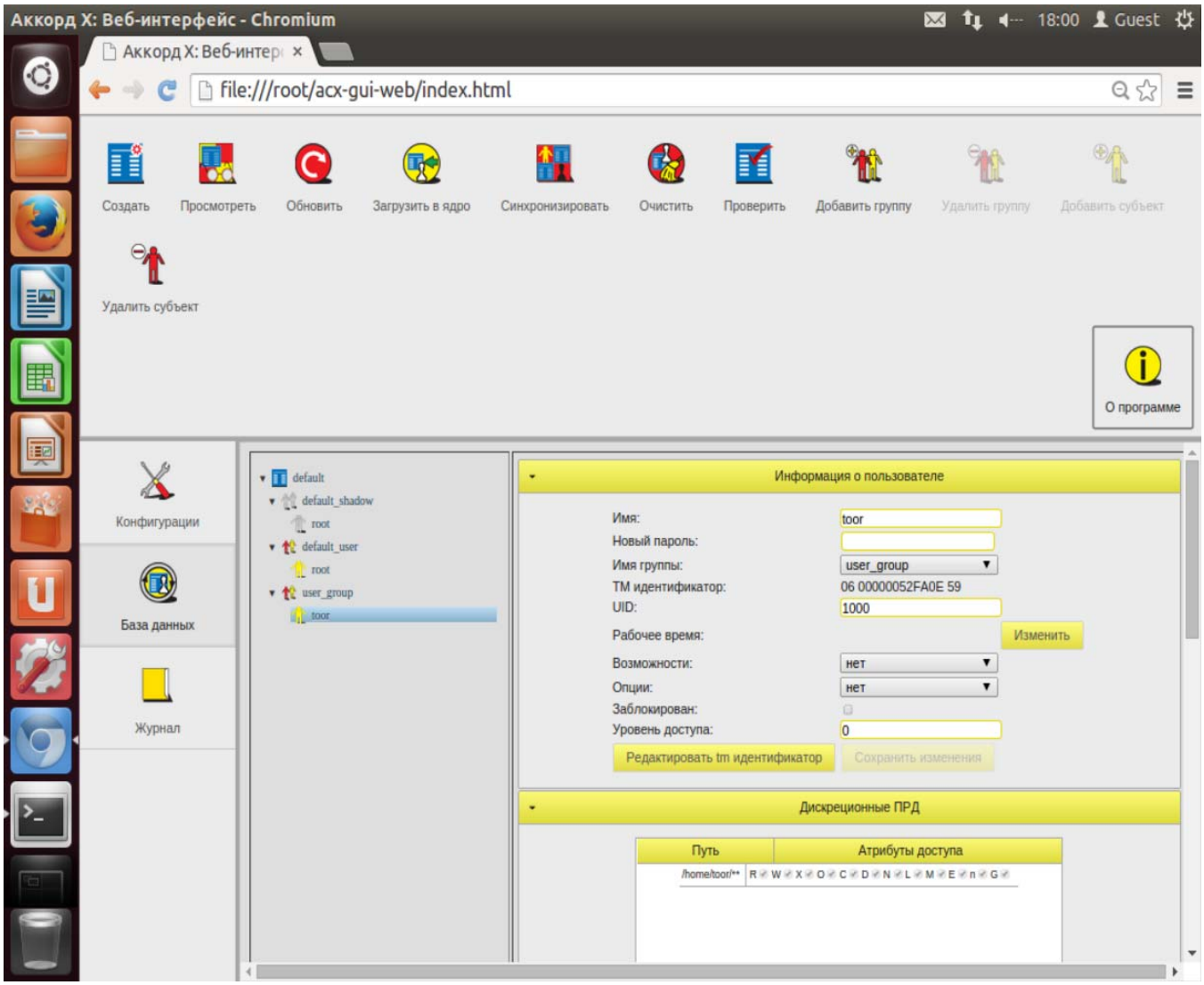

Рисунок 44 - Пользователь с именем toor в базе данных пользователей «Аккорд-X K» (Web-приложение)

5.6 Задание дискреционных прав разграничения доступа

Рассмотрим вопрос задания ПРД для созданных пользователей «Аккорд-X K». Однако стоит иметь в виду, что при установке впервые желательно пропустить следующие пункты с настройкой ПРД/контроля целостности и закончить процесс установки СПО Аккорд-X (чтобы убедиться, что Комплекс работоспособен с отключенными механизмами безопасности или с ПРД, разрешающими все действия).

Итак, после успешного выполнения установки и первичной настройки необходимо задать дискреционные политики разграничения доступа созданным пользователям.

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.

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).

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).

Для задания дискреционных ПРД следует выбрать нужного пользователя из списка, в рабочем поле выбрать пункт «Дискреционные ПРД» и нажать кнопку <Добавить>.

В появившемся далее окне следует указать путь к необходимому каталогу (из ранее созданных), задать для него уровень рекурсии и атрибуты доступа и нажать кнопку <Добавить>.

37222406.26.20.40.140.085 90

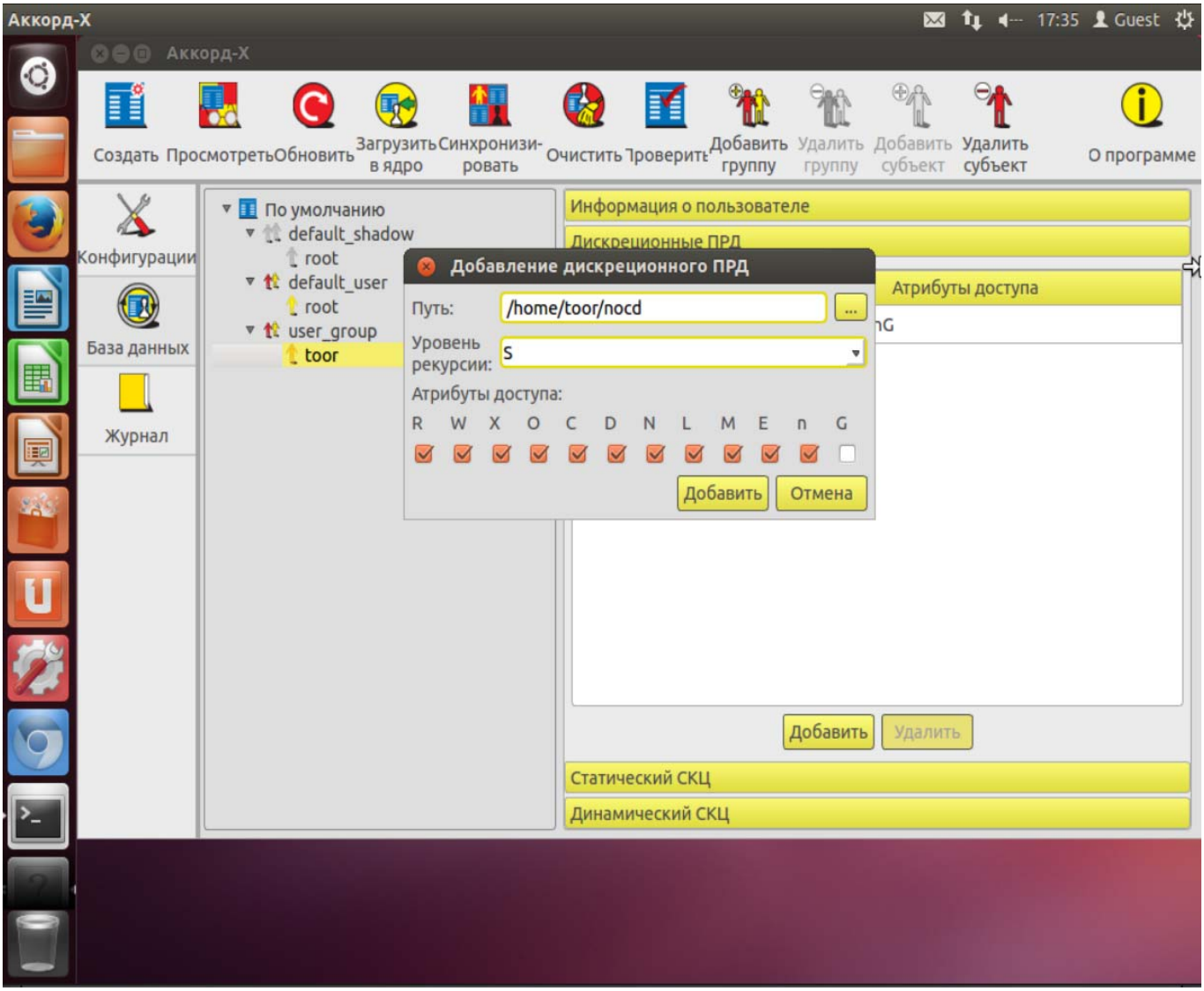

Рисунок 45 - Задание дискреционных ПРД (пользовательское GUI-приложение)

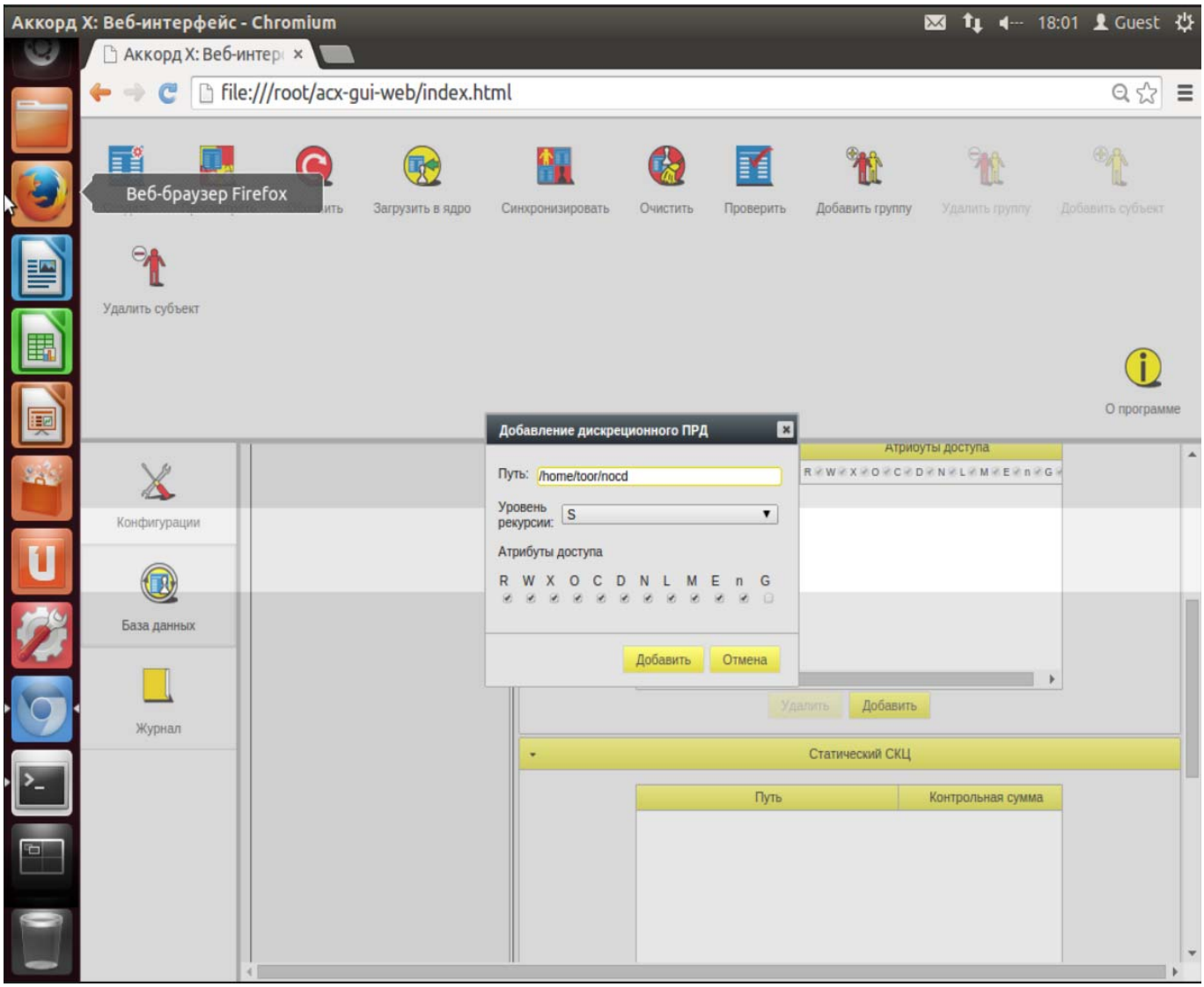

Рисунок 46 - Задание дискреционных ПРД (Web-приложение)

При нажатии кнопки <Добавить> созданные ПРД для выбранного каталога добавляются в базу.

37222406.26.20.40.140.085 90

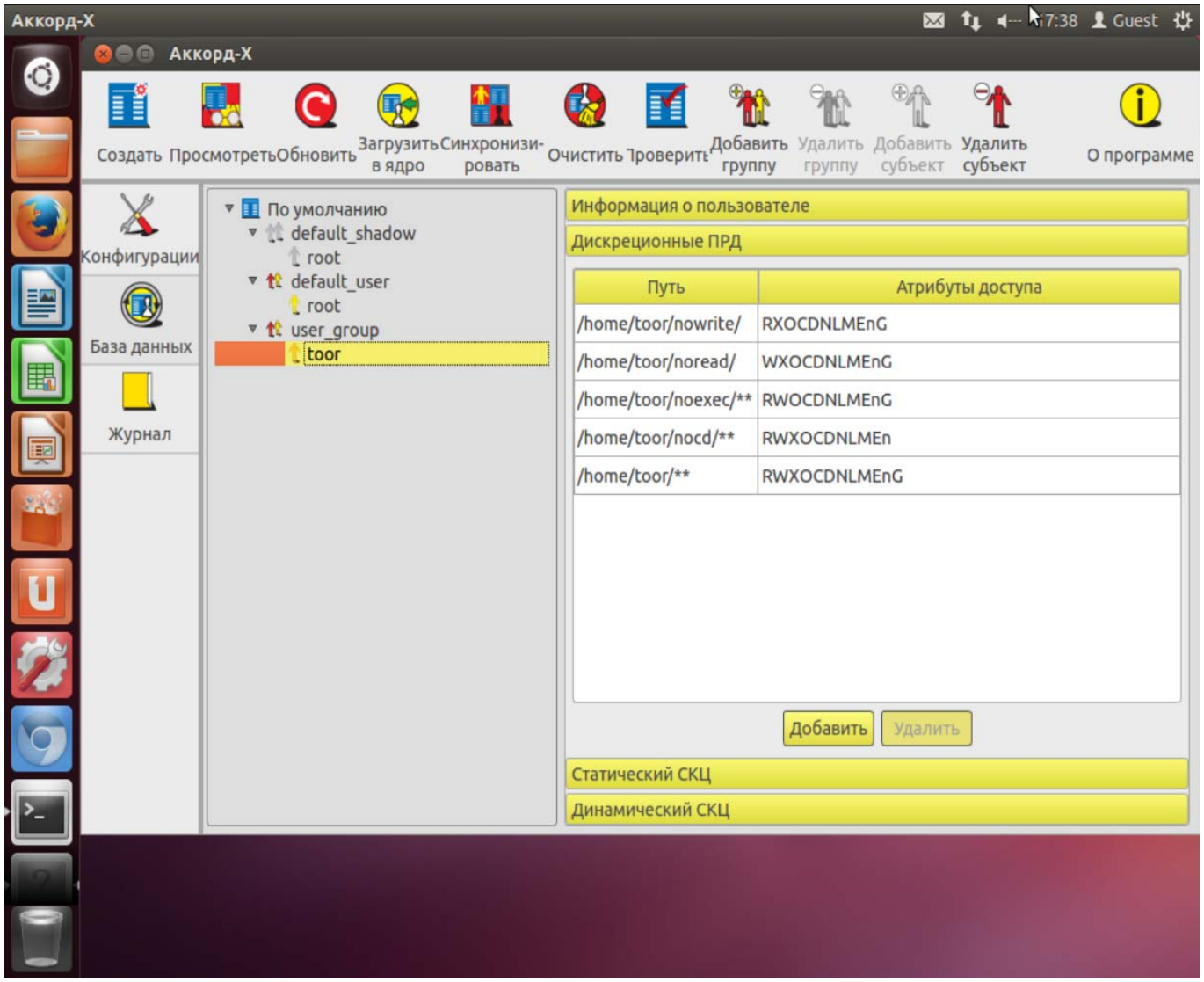

Рисунок 47 - Дискреционные ПРД, заданные пользователю toor (пользовательское GUI-приложение)

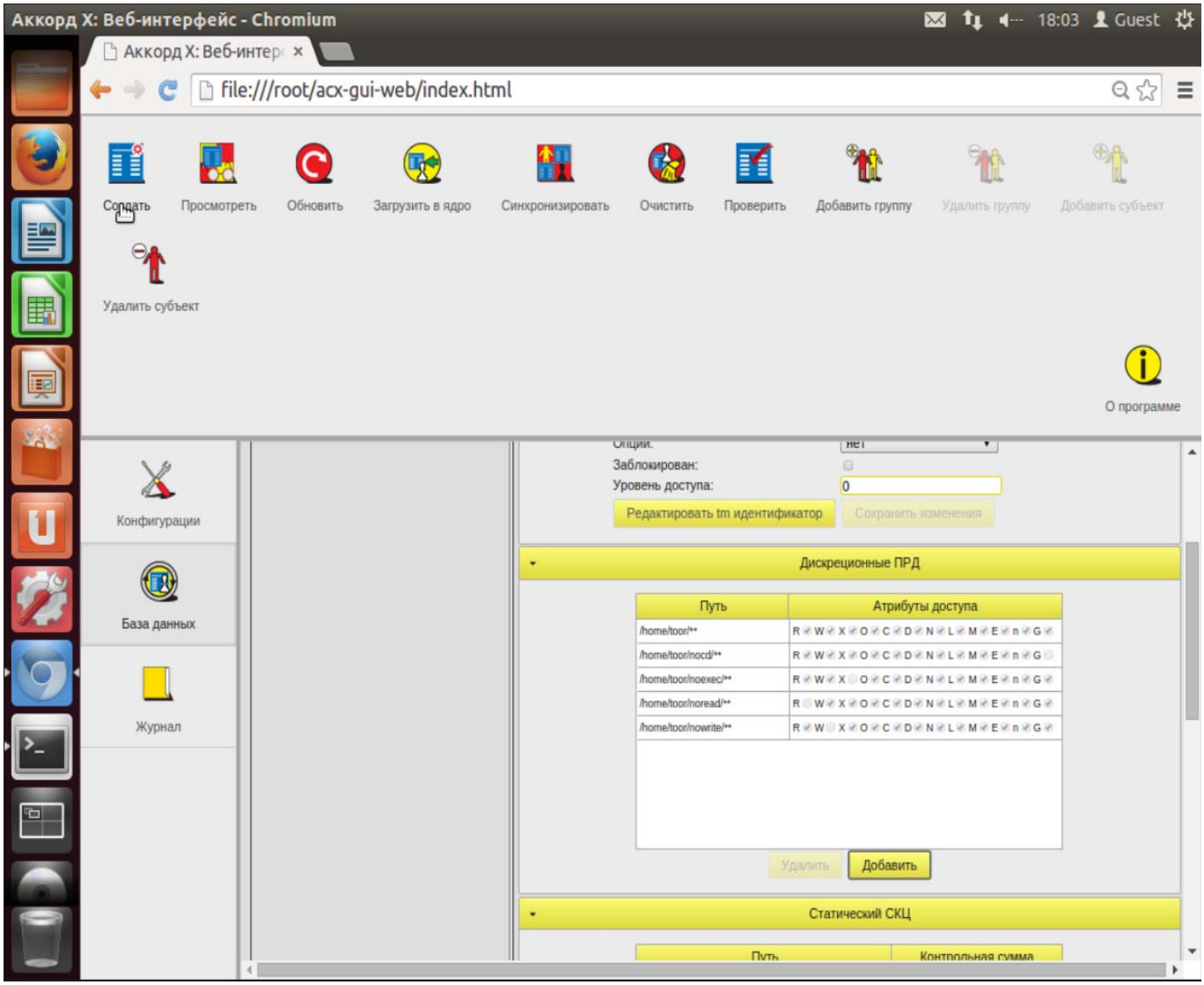

Рисунок 48 - Дискреционные ПРД, заданные пользователю toor (Web-приложение)

5.7 Создание списков контроля целостности

Создание списков контроля целостности (СКЦ) выполняется в рабочем поле для выбранного пользователя на вкладке «База данных». 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.

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).

Пример. Демонстрация заполнения списка динамического контроля целостности.

Создадим бинарный файл (test_bin.sh) и занесем его в динамический список контроля целостности.

Для этого на вкладке «База данных» следует выбрать в списке строку с базой данных (в данном случае строка имеет название «По умолчанию», т.к. при создании файла с БД указан путь по умолчанию).

В появившемся далее окне следует выбрать нужный файл и нажать кнопку <Добавить> (рисунок 49) или <OK> (рисунок 50).

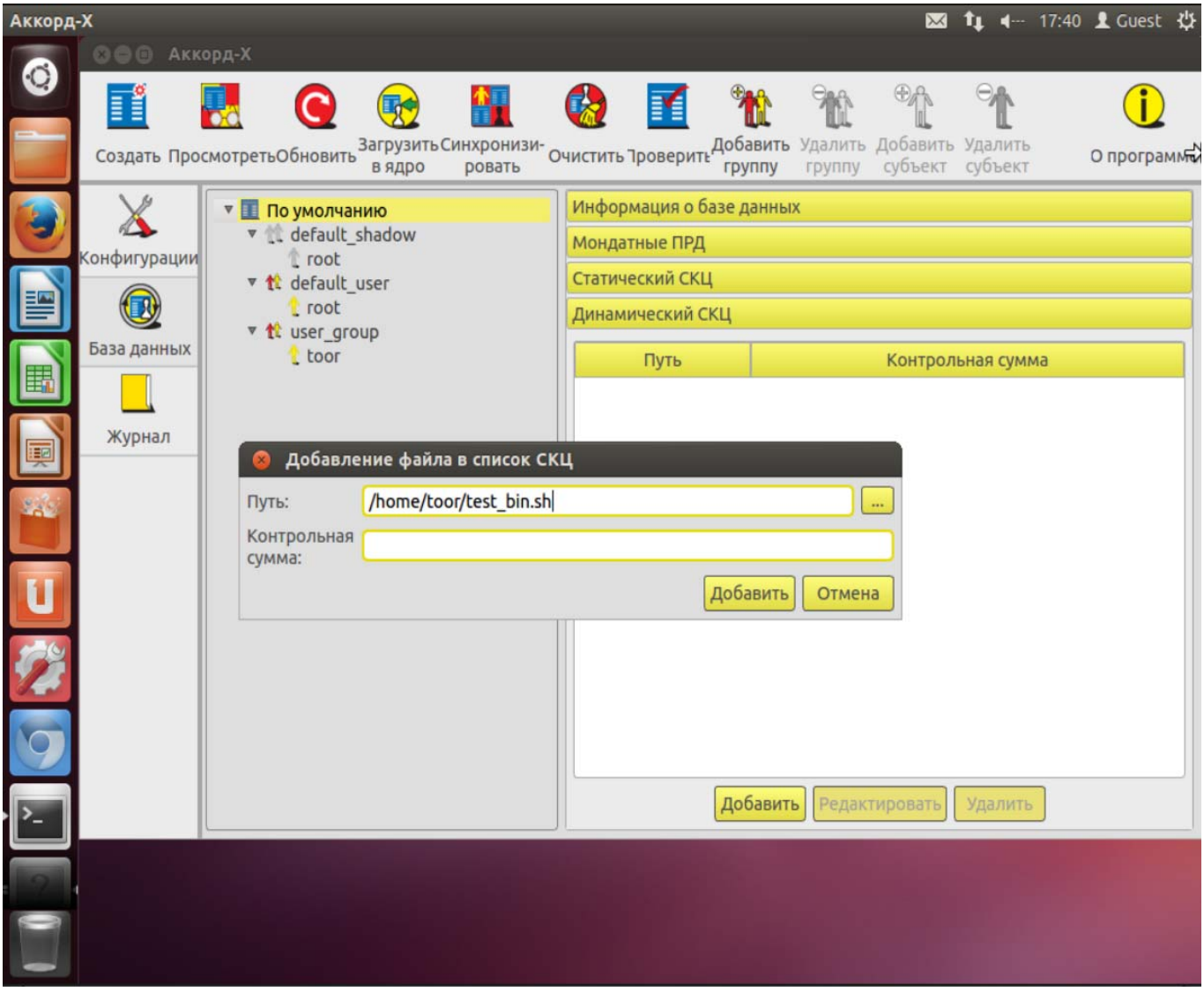

Рисунок 49 - Добавление файла в динамический СКЦ (пользовательское GUI-приложение)

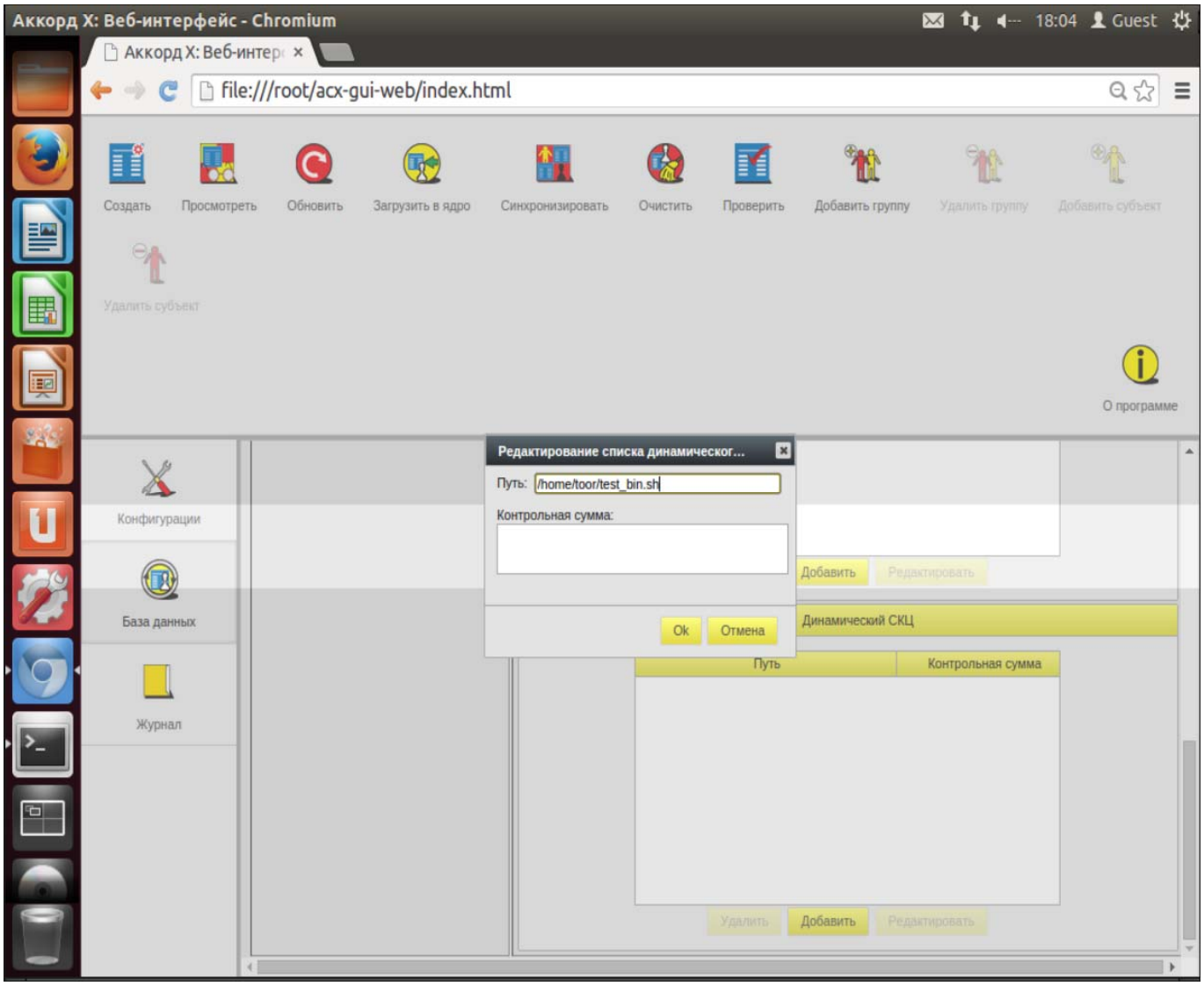

Рисунок 50 - Добавление файла в динамический СКЦ (Web-приложение)

По завершении описанной последовательности действий объект добавляется в динамический СКЦ (рисунок 51).

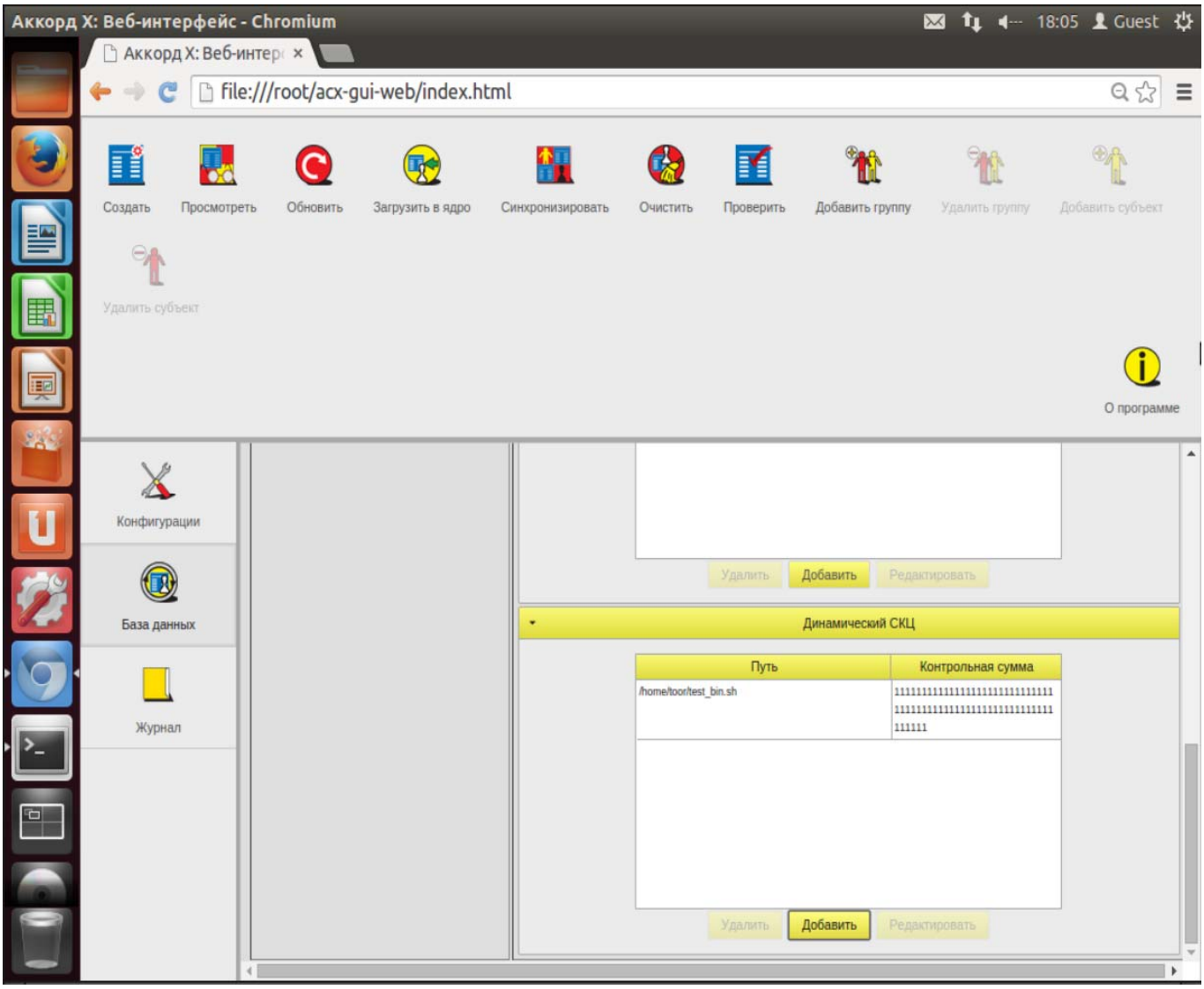

Рисунок 51 - Добавленный в динамический СКЦ файл (Web-приложение)

Статический контроль целостности

Статический контроль целостности осуществляет контроль целостности любых файлов в тот момент, когда запускается утилита **acx-integrity-controller/acx-integrity-controller-db.**

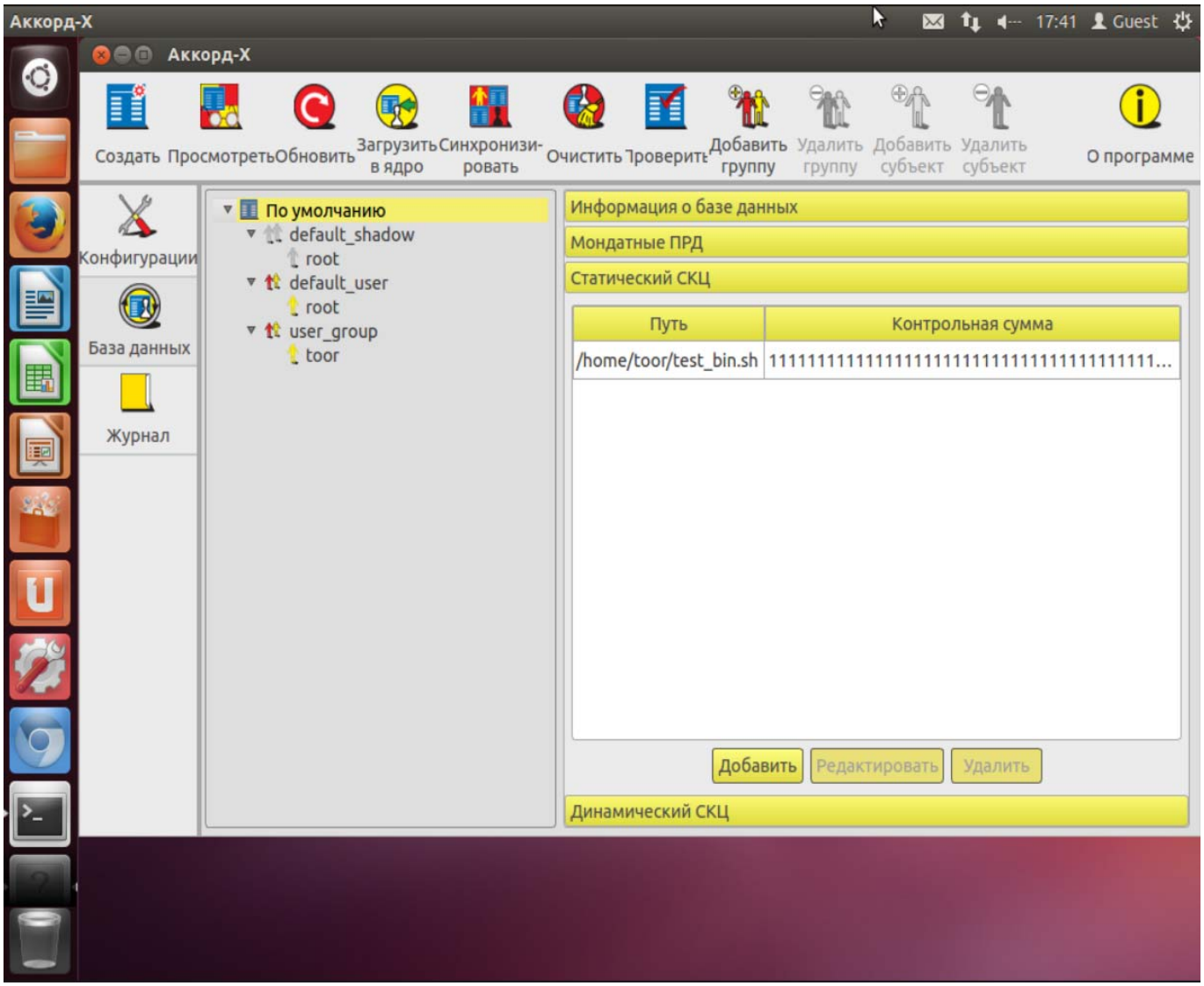

Рисунок 52 - Статический СКЦ (пользовательское GUI-приложение)

5.8 Примеры выполнения установленных ПРД

Пример 1. Демонстрация работы ПРД, когда пользователю запрещено переходить в каталог:

37222406.26.20.40.140.085 90

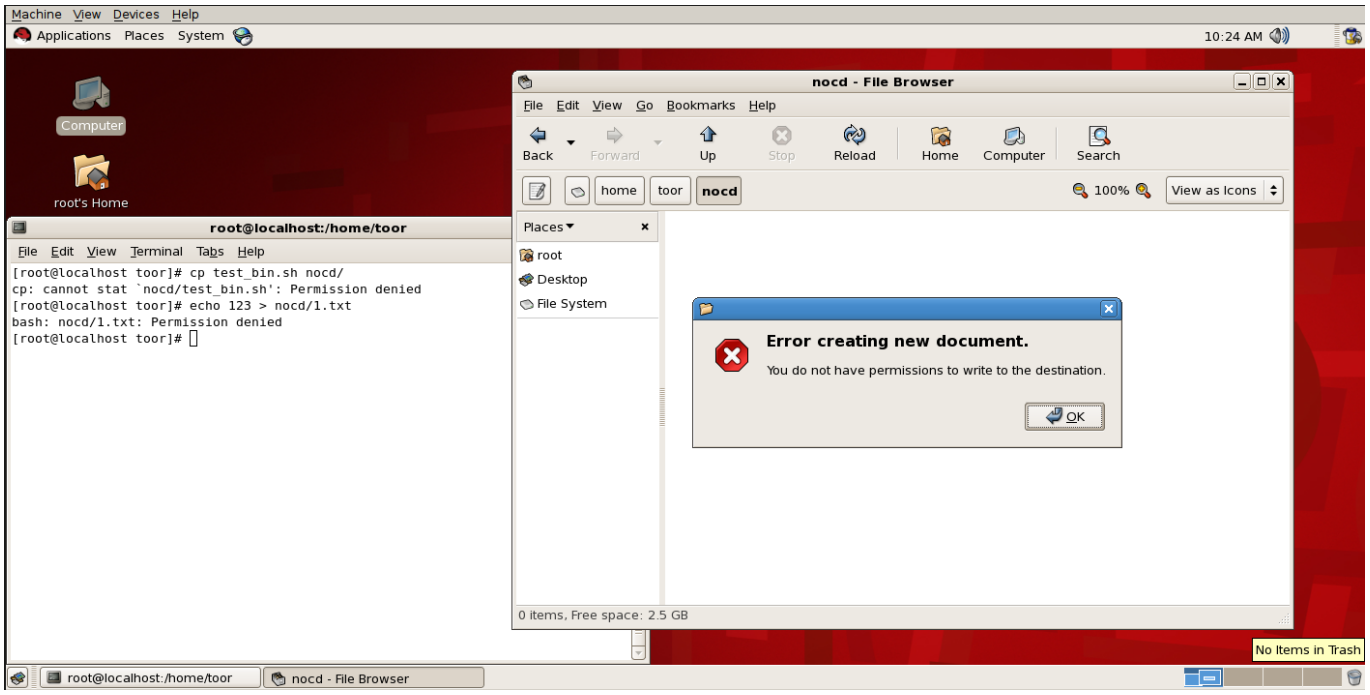

Рисунок 53 – Запрет перехода в каталог

Пример 2. Демонстрация работы ПРД, когда пользователю запрещено открывать на чтение файлы:

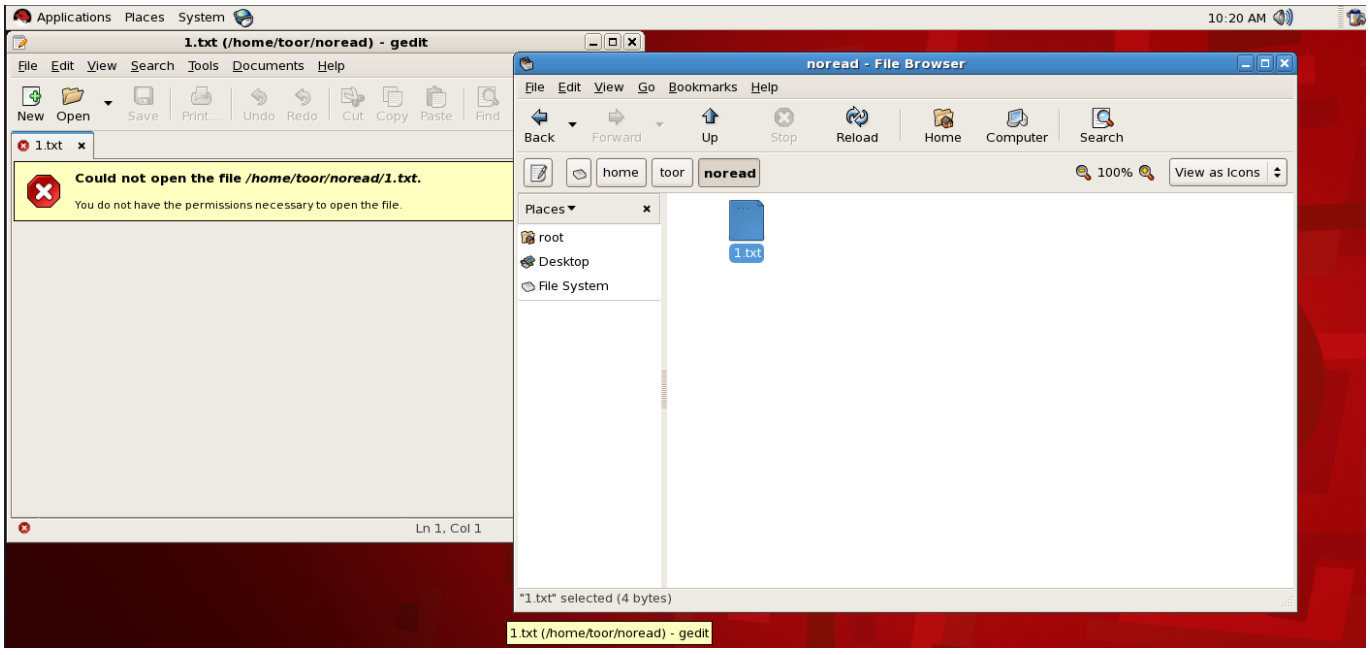

Рисунок 54 – Запрет открытия файлов на чтение

Пример 3. 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); документ имеет статус «read-only», кнопка <Сохранить> недоступна:

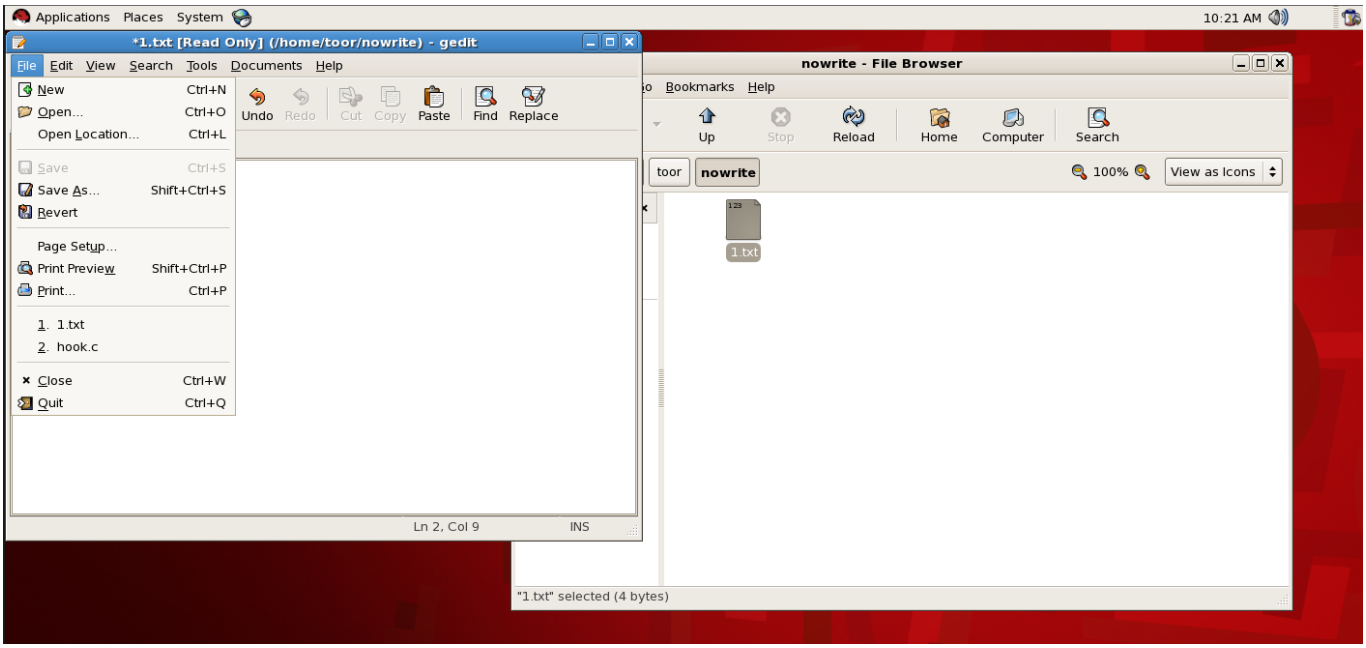

Рисунок 55 - Запрет на запись данных в объект

5.9 Работа с журналом регистрации событий

Работа с журналом осуществляется на вкладке «Журнал» главного окна программы управления.

37222406.26.20.40.140.085 90

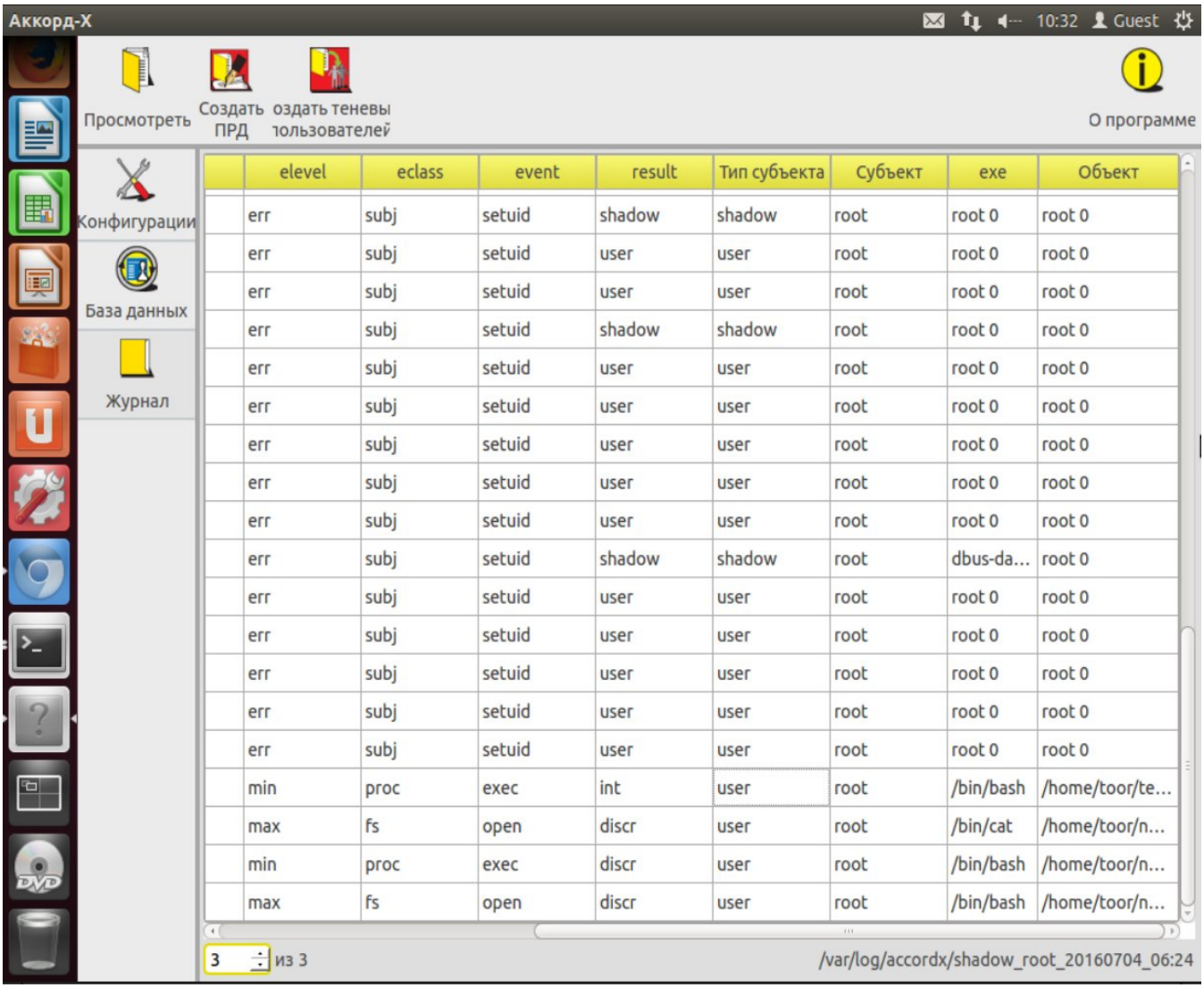

Рисунок 56 - Вкладка «Журнал» (пользовательское GUI-приложение)

37222406.26.20.40.140.085 90

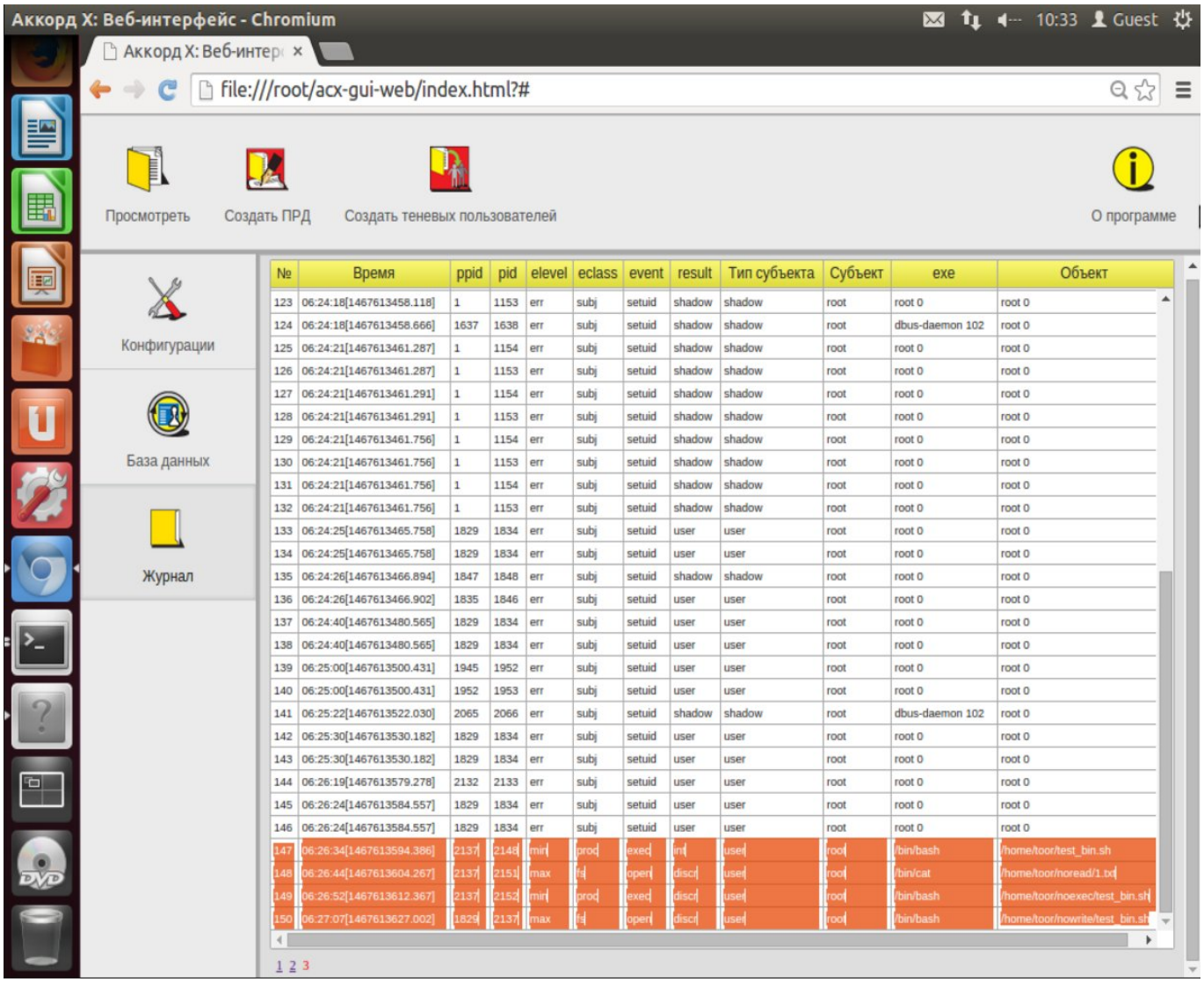

Рисунок 57 - Вкладка «Журнал» (Web-приложение)

6 СНЯТИЕ СРЕДСТВ ЗАЩИТЫ КОМПЛЕКСА «АККОРД-Х»

Снятие (отключение) средств защиты СПО 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 разрешено только Администратору БИ (супервизору).

Для снятия защиты Администратору БИ необходимо отключить подсистему разграничения доступа (перейти на использование штатного initrd ОС), а также удалить или закомментировать внесенные изменения в файлы из /etc/pam.d/.

7 ПРАВОВЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ СПО

СПО «Аккорд-Х К» и сопутствующая документация защищены законом России об авторских правах, а также положениями Международного Договора. Любое использование СПО в нарушение закона об авторских правах или в нарушение положений ЭД на СПО будет преследоваться ОКБ САПР в силу наших возможностей.

Авторские права на данное изделие принадлежат ОКБ САПР, Россия, 115114, г. Москва, 2-й Кожевнический пер., д.12, тел. +7 (926) 762-17-72, E-mail: okbsapr@okbsapr.ru.

ОКБ САПР разрешает Вам делать архивные копии программного обеспечения АККОРД для использования потребителем, приобретшим АККОРД в установленном порядке. Ни при каких обстоятельствах программное обеспечение АККОРД не распространяется между другими предприятиями (фирмами) и лицами.

Удалять в продукции АККОРД уведомление об авторских правах ни при каких обстоятельствах не допускается.

Применение средств комплекса АККОРД для других целей возможно только при наличии письменного согласия ОКБ САПР.

Отметим, что предыдущие ограничения не запрещают Вам распространять Ваши собственные исходные коды или модули, связанные с применением программного обеспечения комплекса АККОРД. Однако, тот, кто получает от Вас такие исходные коды или модули, должен приобрести собственную копию нашего программного обеспечения, чтобы на законном основании использовать его и иметь сертификат соответствия.

ОКБ САПР гарантирует исправность физических экземпляров аппаратуры и документации, поставляемых в составе комплекса АККОРД, согласно Формуляру на этот Комплекс.

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

Комплекс АККОРД поставляется по принципу «as is», т.е. ОКБ САПР ни при каких обстоятельствах не предусматривает никакой компенсации за Ваши дополнительные убытки, включая любые потери прибыли, потери сохранности или другие убытки вследствие аварийных ситуаций или их последствий, убытки, которые могут возникнуть из-за использования или невозможности использования комплекса АККОРД. Тем не менее, любые Ваши потери могут быть возмещены в том случае, если Вы оформите страховой полис по разделу «Страхование информационной безопасности». Страховка оформляется по Вашему требованию непосредственно у поставщика.

При покупке и применении комплекса АККОРД предполагается, что Вы знакомы с данными требованиями авторов разработки и изготовления комплекса АККОРД и согласны с положениями настоящего раздела.

8 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

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

+7 (495) 994-49-96

+7 (495) 994-49-97

+7 (926) 762-17-72

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

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

ПРИЛОЖЕНИЕ 1. 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 (АБИ).

Сотрудники СБИ (АБИ) 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 (АБИ):

- СБИ (АБИ) должны подчиняться тому лицу, которое в данной организации несет персональную ответственность за соблюдение правил обращения с защищаемой информацией;
- сотрудники службы (АБИ) 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 (АБИ) должно быть предоставлено право запрещать включение в число действующих новые элементы компонентов АС, если они не отвечают требованиям защиты информации;
- службе БИ (АБИ) должны обеспечиваться все условия, необходимые для выполнения своих функциональных обязанностей;
- численность службы должна быть достаточной 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 комплексов СЗИ НСД «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-Х К»:

1. На основе «Плана защиты», введенного в организации, разрабатывать таблицы разграничения доступа к защищаемым ресурсам, вводить полномочия пользователей и корректировать их в ходе эксплуатации СВТ.

2. Устанавливать Комплекс защиты в СВТ и организовывать его 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.

ВНИМАНИЕ!

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 Комплекса и оказывать помощь в части организации работы на СВТ с внедренным Комплексом защиты.

5. Контролировать на целостность (на уровне контроллера) файлы СПО разграничения доступа.

6. Выявлять возможные каналы НСД к информации при применении Комплекса, готовить предложения по их устранению.

7. Систематически анализировать состояние Комплекса и его отдельных средств, периодически проводить их тестирование и проверку защитных функций Комплекса, о чем делать отметку в Формуляре.

8. Регулярно анализировать содержание системного журнала и разрабатывать меры по исключению неправильного применения Комплекса пользователями.

ВНИМАНИЕ!

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 (журнал учета идентификаторов, 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, комплекс с эксплуатации, о чем делать отметку в Формуляре.

12. Принимать меры при попытках НСД к защищаемой информации и нарушении правил функционирования системы защиты. Обязанности АБИ

должны быть отражены в «Инструкции администратора безопасности информации», утвержденной соответствующим должностным лицом.

13. В случае выявления сбоев и ошибок в процессе эксплуатации изделия АБИ обязан:

- произвести верификацию СПО «Аккорд-X K» в соответствии с инструкцией по верификации приведенной в формуляре (37222406.26.20.40.140.085 ФО);
- если ошибок при верификации не выявлено, то необходимо перезапустить СВТ и продолжить эксплуатацию изделия;
- при выявлении ошибки при верификации изделия, необходимо прекратить эксплуатацию изделия и обратиться за консультацией разработчику.

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 или АМДЗ, 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) `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);
7) `icl` - списками контроля целостности (формат 'объект ~ контрольная сумма');
8) `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 или изменение данных в БД-

Команда	Опции/параметры команды	Комментарий
		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)
	--no-auth, -n	с помощью данной опции можно работать с БД Аккорд-АМДЗ без прохождения процедуры идентификации/аутентификации при каждом изменении (только один раз вначале)
	-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 XXXXXXXXXXX XX'	задать ТМ-идентификатор (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 на основе иерархических меток
	-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, tm 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
	-O	указание на то, что требуется автоматически создавать пользователя в БД ОС
	-n	указание на то, что вместо аппаратных идентификаторов планируется использовать вход по логину (и паролю)
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 ТМ-идентификатор (влечет изменение xid). Если изменился только ТМ - дополнительно запрашивается пароль

Команда	Опции/параметры команды	Комментарий
		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 на основе иерархических меток
	-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
	-O	указание на то, что требуется автоматически изменять пользователя и в БД ОС и в БД «Аккорд-Х»
	-n	указание на то, что вместо аппаратных идентификаторов планируется использовать вход по логину (и паролю)
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
	-O	указание на то, что требуется автоматически удалять пользователя из БД ОС
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
	-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 acl

`acx-admin acl` - утилита для работы с правилами разграничения доступа субъектов к объектам. Основные команды и опции данной утилиты описаны в таблице 5.

Таблица 5 - Основные команды и опции acx admin acl

Команда	Опция/параметр	Комментарий
show		Вывести на экран правила разграничения доступа или уровни доступа на основе иерархических меток, 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.
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		Задать уровень конфиденциальности для объекта доступа[2], при этом:

[1)] Данный формат команды позволяет задать правила в рамках дискреционного контроля доступа, т.е. для каждого субъекта доступа (пользователя, shadow) 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)

Команда	Опция/параметр	Комментарий
№ 2)[1]	--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 доступа[3]. 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 6.

---

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

[1] Данный формат команды позволяет задать правила в рамках контроля доступа на основе иерархических меток, то есть 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.

[3] В качестве параметра необходимо передать либо объект доступа, либо номер правила в списке ACL.

Таблица 6 – 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 show		Вывести СКЦ пользователя или группы
	-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 7.

Таблица 7 - Основные команды и опции acx admin log

Команда	Опция/параметр	Комментарий
acx-admin log show		Просмотр содержимого log-файла
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 К» 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 отсчета 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 8);
- результат – в таблице выводится краткая аббревиатура (подробное описание см. в таблице 9);
- тип субъекта, от имени которого осуществляется доступ (user, shadow, process);
- имя субъекта доступа (имя берется из БД Аккорд-X);
- 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 8 - 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 9 – Результаты операций, регистрируемые в журнале

Аббревиатура	Значение
Операции с доступом к объектам	
ok	событие не нарушило ПРД Аккорд-X, операция разрешена, setuid разрешен
discr	доступ запрещен дискреционной политикой
mand	доступ запрещен политикой на основе иерархических меток
int	нарушена целостность объекта при контроле целостности динамического СКЦ
oserr	произошла ошибка ОС
seterr	произошла ошибка, связанная с settings
Операции смены субъекта доступа (setuid)	
ok	setuid разрешен
user	setuid на пользователя user разрешен (аналог ok, с указанием дополнительной информации)
shadow	setuid на пользователя shadow разрешен (аналог ok, с указанием дополнительной информации)
wuid	произошла ошибка - в ходе setuid использован неправильный UID
nauth	произошла ошибка - попытка setuid на пользователя user без идентификации и аутентификации
noshadow	произошла ошибка - в ходе setuid отсутствует пользователь shadow с заданным UID
nrability	произошла ошибка - пользователю shadow запрещено делать setuid на 0
nability	произошла ошибка - пользователю shadow запрещено делать setuid
Операции входа/выхода пользователя	
pamerr	произошла ошибка в PAM
nouser	произошла ошибка - отсутствует пользователь user с заданным UID
wxid	произошла ошибка - идентификатор или пароль введены некорректно
retryerr	произошла ошибка - превышено количество некорректных попыток входа
autherr	произошла другая ошибка аутентификации
multilogin	произошла ошибка - пользователю нельзя создавать более одной сессии
logoutnouser	произошла ошибка в PAM при выходе пользователя, пользователь с таким UID не найден
logoutpamerr	произошла другая ошибка в PAM при выходе пользователя
logouterr	произошла другая ошибка при выходе пользователя

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

Требования для поддержки смарт-карт и токенов:

- необходимые зависимости: как минимум pcsc-lite, ccid (libccid). 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;
- на некоторых ОС необходимо отключить автозапуск openct (из-за конфликта с libccid и т.п.), например, в RHEL:

1. chkconfig --list | grep openct [см. уровни, где openct включен]
2. chkconfig --level 2 openct off
3. chkconfig --level 3 openct off
4. chkconfig --level 4 openct off
5. chkconfig --level 5 openct off

- необходимо добавить в файл конфигурации /usr/lib/pcsc/drivers/ifd-acsccid.bundle/Contents/Info.plist (для карт и считывателей ACS) или /usr/lib/pcsc/drivers/ifd-ccid.bundle/Contents/Info.plist (для устройств ШИПКА; например **0x17e4/0x0040** для ШИПКА лайт slim) 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>
</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>
</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>
</array>

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

ПРИЛОЖЕНИЕ 5. Рекомендации по реализации мер безопасной настройки среды исполнения СПО «Аккорд-X K»

В рамках реализации мер по безопасной настройке среды исполнения СПО «Аккорд-X K» рекомендуется динамически (статически) в процессе работы ОС GNU/Linux или до ее загрузки осуществлять контроль целостности компонент, перечисленных в таблице 10, а также осуществлять разграничение доступа к объектам в соответствии с данными из таблицы 11.

Для формирования правил доступа и списков контроля целостности в соответствии с таблицами 10 и 11 по запросу Пользователя Разработчик предоставляет скрипт безопасной настройки *acx-secure-setup.s*h. Скрипт необходимо запускать после установки и настройки комплекса с помощью команды "*/bin/acx-secure-setup.sh*". В случае успешного пополнения списков контроля доступа и целостности будет выведена информация, аналогичная следующей:

...
added '/usr/sbin/zramctl'
Database dumped into /etc/accordx/db.json successfully
Global dynamic ICL: 13424 object(s)

AccordX is configured securely!

Для проверки того, что конфигурация среды исполнения «Аккорд-X K» является безопасной необходимо использовать команду "*/bin/acx-secure-setup.sh check*". В случае если проверка завершается успешно выводится информация, аналогичная следующей:

...
/usr/sbin/zramctl -> OK
ICL list is complete
Global dynamic ICL: 13424 object(s)

AccordX is configured securely!

В случае возникновения ошибок выводится информация, аналогичная следующей:

...
ICL list is incomplete or the integrity of some objects is violated

AccordX is NOT configured securely!
Check for errors in the output above...

В последнем случае необходимо проверить весь вывод "*/bin/acx-secure-setup.sh check 2>&1 > acx-secure.log*" на наличие ошибок. В выводе возможны следующие обозначения для ошибок:

1. /bin/date -> integrity error
2. /bin/date -> failed
3. /bin/date -> not found
4. error: object '/bin/date' not exists in ICL

В случае возникновения ошибок для консультаций необходимо обратиться к Разработчику.

Таблица 10 – Контроль целостности компонент

Объект контроля целостности	Примечание
1. Файлы конфигурации и критичные данные ОС	В зависимости от используемого дистрибутива GNU/Linux и набора используемого ПО, необходимо контролировать целостность следующих компонент: /bin/**[1]; /boot/** (ядро, образ начальной загрузки, загрузчик и его файлы конфигурации); /etc/**; /lib/**[2]; /lib64/**[3]; /sbin/**; /usr/bin/**; /usr/lib/**[4]; /usr/lib64/**[3]; /usr/libexec/**; /usr/sbin/**; /usr/local/bin/**; /usr/local/lib/**; /usr/local/lib64/**[3]; /usr/local/sbin/**. Целостность некоторых описанных компонент необходимо проверять до загрузки ОС (опционально), либо посредством возможности контроля их целостности средствами подсистемы управления доступом (статический или динамический контроль

[1] Обозначения здесь и далее: «**» – все вложенные файлы и каталоги, «*» – любые символы в имени

[2] /lib32/** для 64-разрядных ОС GNU/Linux с поддержкой multilib

[3] для 64-разрядных ОС GNU/Linux

[4] /usr/lib32/** для 64-разрядных ОС GNU/Linux с поддержкой multilib

	целостности). В число указанных объектов также включены: /bin/login, /bin/su, /usr/bin/sudo, /usr/sbin/sshd, /etc/pam. d/**, /lib/security/** или /lib64/security/**, /etc/passwd, /etc/shadow и некоторые другие,а также бинарные файлы системных сервисов.
2. Настройки используемой подсистемы управления доступом	Файлы конфигурации /etc/accordx/**, /usr/lib[1]/cups/filter/accord.cnf. Утилиты администрирования, драйверы и прочие компоненты СПО «Аккорд-X K»: /bin/acx-*; /lib[5]/acx-core.ko; /lib[5]/modules/$(uname-r)[1]/kernel/drivers/usb/serial/shipka.ko; /lib[5]/modules/$(uname-r)[1]/kernel/drivers/usb/serial/shipka_kc2.ko; /lib[5]/modules/$(uname-r)[1]/kernel/drivers/usb/serial/shipka_kc3.ko; /lib[5]/modules/$(uname-r)[1]/kernel/drivers/usb/serial/tmusb_drv.ko; /lib[5]/security/pam_acx*; /usr/bin/acx-admin*; /usr/bin/acx-config; /usr/bin/acx-remote*; /usr/lib[5]/libacx-*; /usr/lib[5]/libosci*; /usr/lib[5]/libtmid*; /usr/lib[5]/tmid-*.

Таблица 11 – Разграничение доступа к объектам

Объект контроля доступа	Права доступа
1. /**	RXCNLMnG[2]
2. /bin/acx-*	–
3. /bin/acx-integrity-controller	RX
4. /bin/acx-integrity-controller-db	RX
5. /boot/**	–
6. /dev/null	RW
7. /etc/	RCNL
8. /etc/mtab*	RWCD
9. /etc/accordx/**	–
10. /etc/accordx/db.json	R
11. /home/$USER[3]/**	RWXCDNLMEnG
12. /lib[4]/acx-core.ko	–
13. /lib[4]/modules/$(uname-r)[1]/kernel/drivers/usb/serial/shipka*	–
14. /lib[4]/modules/$(uname-r)[1]/kernel/drivers/usb/serial/tmusb_drv.ko	–
15. /lib[4]/security/pam_acx*	R
16. /run/**	RWXCDNLMEnG
17. /tmp/**	RWXCDNLMEnG
18. /usr/bin/acx-admin*	–
19. /usr/bin/acx-config*	–
20. /usr/bin/acx-admin	RX
21. /usr/bin/acx-admin-log	RX
22. /usr/lib[4]/cups/filter/accord*	R

[1] lib64 для 64-разрядных ОС GNU/Linux

[2] Обозначения атрибутов доступа: **R/W/X** – чтение, запись, исполнение; **C/D/N** – создание, удаление, переименование; **L** – создание ссылки; **M/E/n** – создание, удаление, переименование каталога; **G** – переход в каталог.

[3] имя пользователя

[4] lib64 для 64-разрядных ОС GNU/Linux

23. /usr/lib[4]/cups/filter/accord.users/**	RG
24. /usr/lib[4]/libacx-core*	–
25. /usr/lib[4]/libacx-db*	R
26. /usr/lib[4]/libacx-log*	R
27. /usr/lib[4]/libacx-print*	R
28. /usr/lib[4]/libosci*	R
29. /usr/lib[4]/libtmid*	R
30. /usr/lib[4]/tmid*	R
31. /var/log/accordx/**	RG