УТВЕРЖДЕН

ЦАУВ.14001-01 91 01-ЛУ

Клиентская операционная система с интегрированными пользовательскими приложениями МСВСфера 6.3 АРМ

Руководство администратора

ЦАУВ.14001-01 91 01

Версия 1.0

2013

Изм.	Лист	№ докум	Подп	Дата

АННОТАЦИЯ

Настоящее руководство предназначено для администраторов клиентской операционной системы с интегрированными пользовательскими приложениями МСВСфера 6.3 АРМ.

В нем представлено описание последовательности действий, необходимых для установки и обновления системы, рассмотрены функциональные возможности встроенных средств защиты информации, порядок их настройки и использования.

СОДЕРЖАНИЕ

Изм.	Лист	№ докум	Подп	Дата

1 ВВЕДЕНИЕ

МСВСфера 6.3 АРМ – это интегрированное программное решение, включающее в себя надежную и быструю клиентскую операционную систему на базе ядра Linux со встроенными средствами защиты информации и большой набор пользовательских приложений.

МСВСфера 6.3 АРМ предназначена для создания многофункциональных автоматизированных рабочих мест. Для этого в ее состав входят пользовательские приложения следующих групп:

- программы для обработки офисных документов;
- программы управления персональной информацией;
- программы электронной почты и обмена сообщениями;
- приложения для телефонии и видеоконференций;
- программы управления проектами и заметками;
- веб-браузеры и менеджеры файлов и архивов;
- редакторы текстов, графики и бинарных данных;
- программы воспроизведения аудио и видео;
- программы для записи оптических дисков;
- среды разработки и средства моделирования;
- архиватор, калькулятор и другие приложения.

МСВСфера 6.3 АРМ совместима с большим числом современных аппаратных платформ на базе 64-х разрядных процессоров Intel и AMD. Для установки и работы МСВСфера 6.3 АРМ требуется компьютер со следующими минимальными характеристиками:

- 64-х битный процессор Intel или AMD;
- 1024 MB оперативной памяти;
- 10 GB свободного пространства на жестком диске;
- устройство чтения DVD-дисков.

2 УСТАНОВКА И ОБНОВЛЕНИЕ СИСТЕМЫ

2.1 Установка системы

Для установки МСВСфера 6.3 АРМ необходимо выполнить следующую последовательность действий*.

1. Вставьте DVD-диск с инсталляционным дистрибутивом МСВСфера 6.3 АРМ в устройство чтения данных с оптических дисков и осуществите загрузку с него.

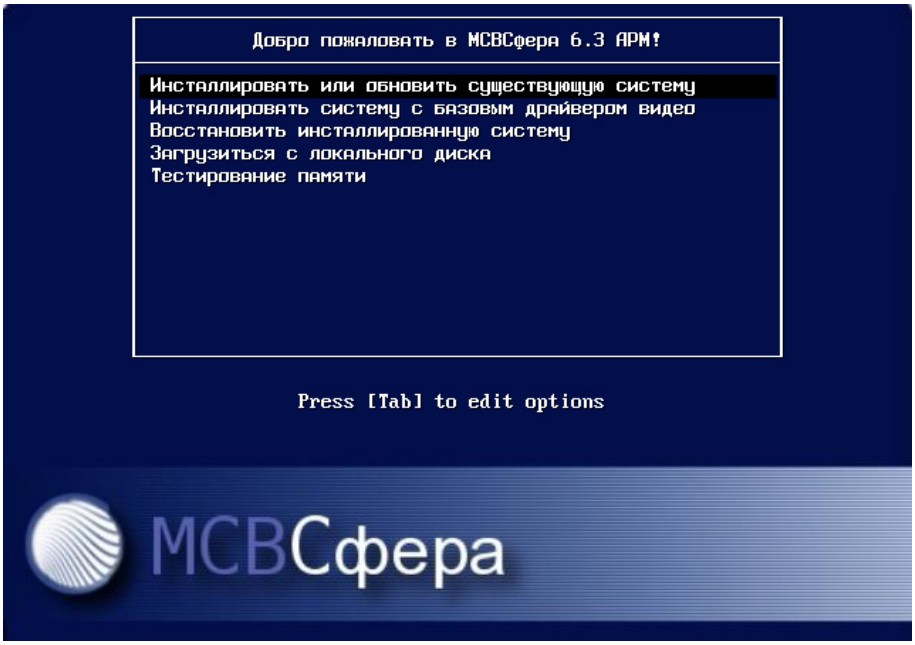


Рисунок 1 – Загрузка системы с диска

* Перед началом установки или обновления системы рекомендуется предварительно ознакомиться с процедурами контроля целостности программной среды, описанными в разделе 10.

2. Первоначальная загрузка проходит в текстовом режиме. На экране отобразятся сообщения о загрузке отдельных модулей установочной системы.

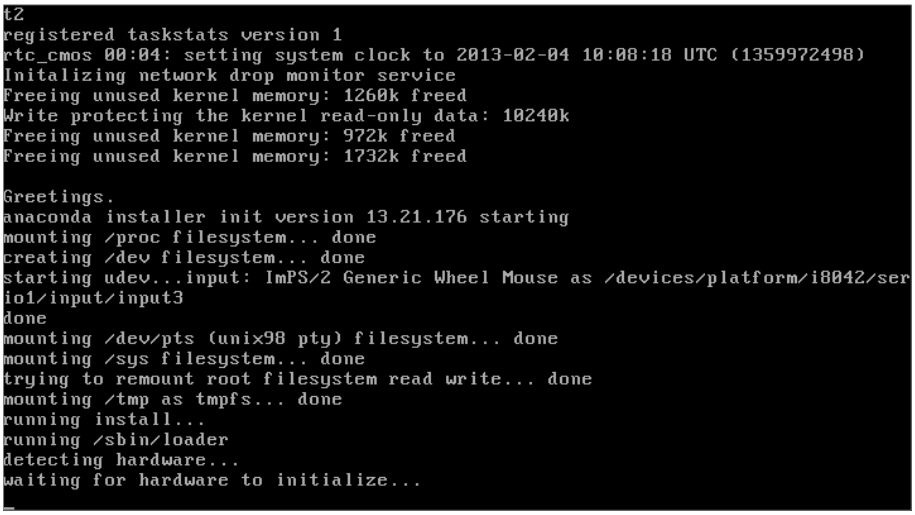


Рисунок 2 – Загрузка модулей системы

3. Затем система предложит сделать проверку целостности установочного диска. При необходимости сделать проверку следует выбрать и нажать кнопку «OK», для продолжения установки следует выбрать и нажать кнопку «Skip».

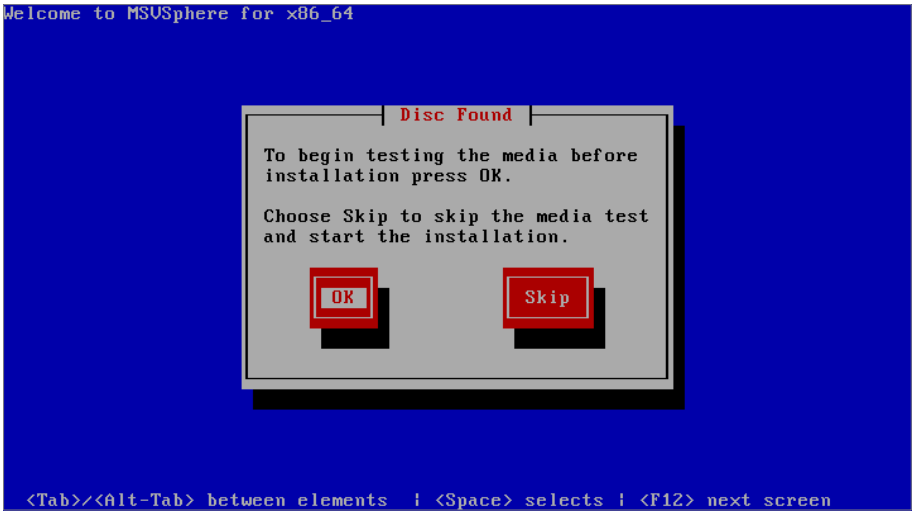


Рисунок 3 – Проверка целостности установочного диска

Изм.	Лист	№ докум	Подп	Дата

4. Для того чтобы начать проверку, нужно выбрать и нажать кнопку «Test».

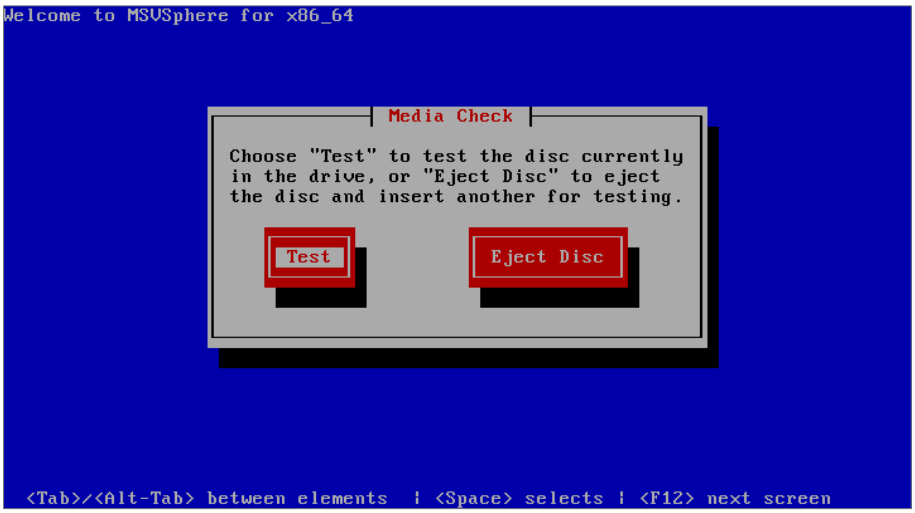


Рисунок 4 – Начало проверки

5. На экране появится следующее сообщение.

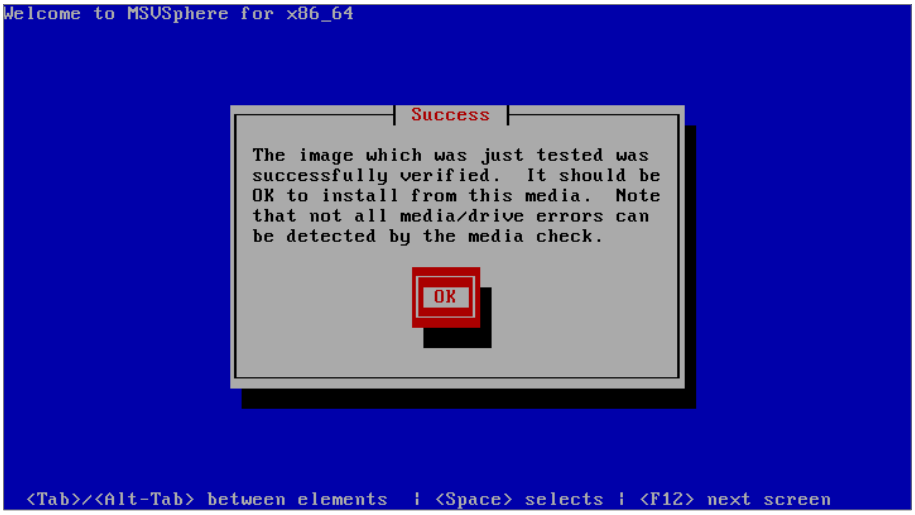


Рисунок 5 – Окно-предупреждение

6. Для продолжения процесса установки необходимо вставить DVD-диск в устройство чтения и нажать кнопку «ОК».

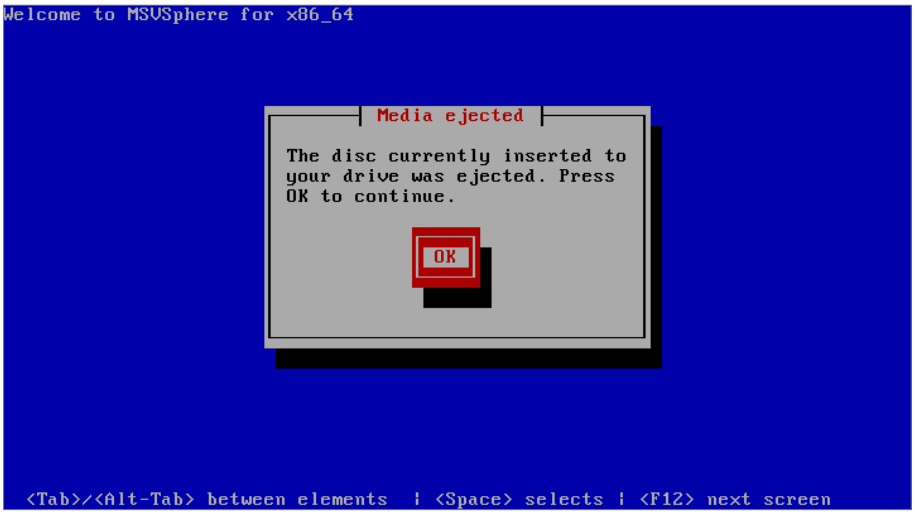


Рисунок 6 – Сообщение о необходимости вставить диск в DVD-ROM

7. Установочная система загрузит графический модуль.

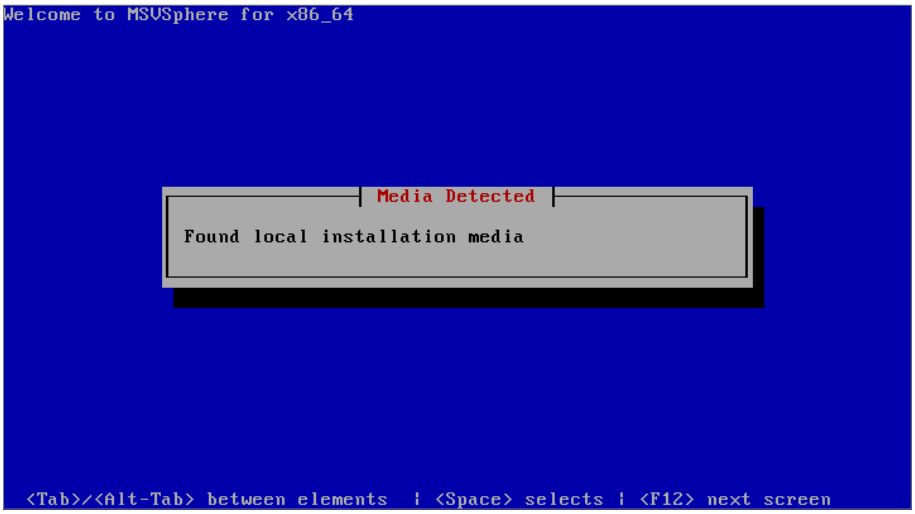


Рисунок 7 – Загрузка графического модуля

8. После этого установочная система перейдет в графический режим работы.

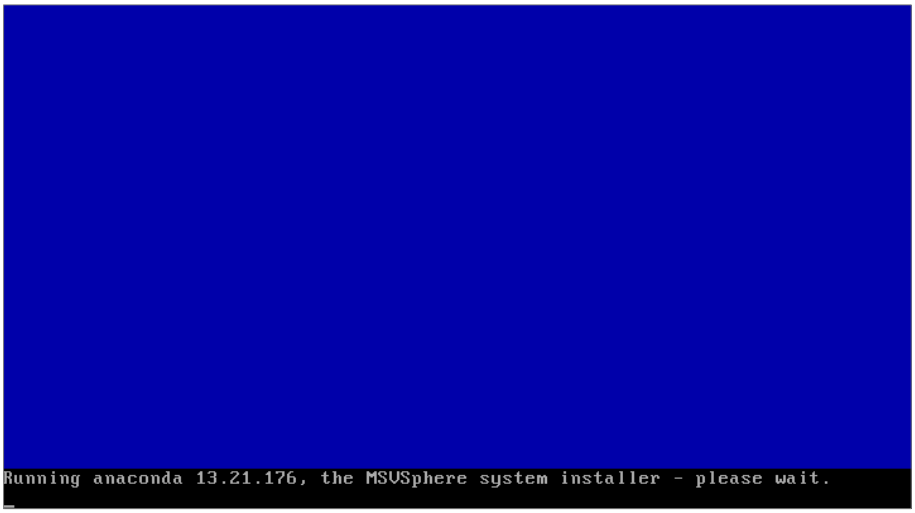


Рисунок 8 – Графический режим работы

9. Когда появится экран приветствия, нажмите кнопку «Next».

Рисунок 9 – Экран приветствия

10. Система предложит выбрать язык. Выбрав язык, нажмите «Next».

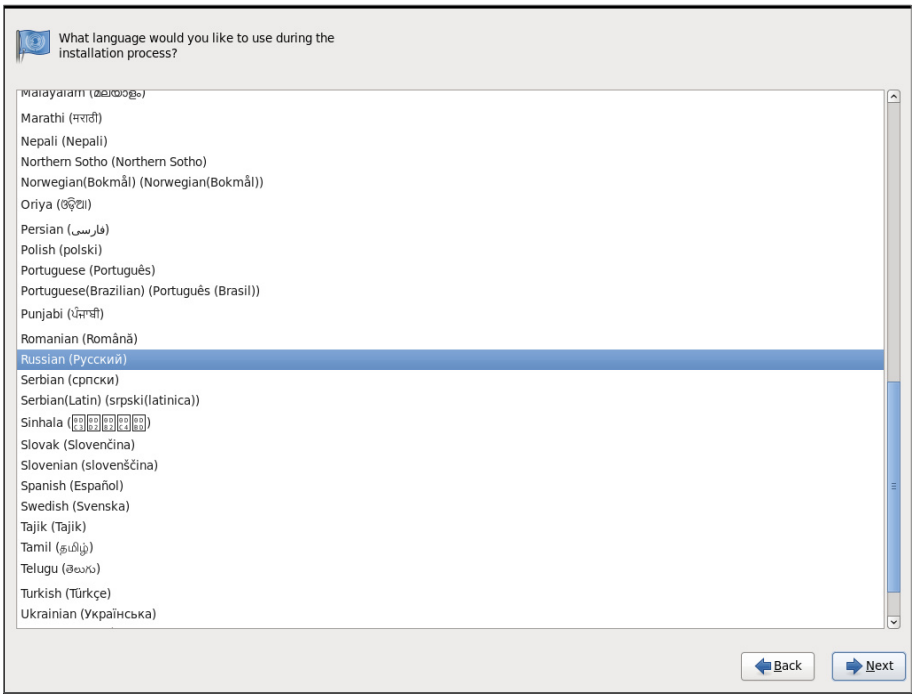


Рисунок 10 – Выбор языка

11. После этого будет предложено выбрать раскладку клавиатуры.

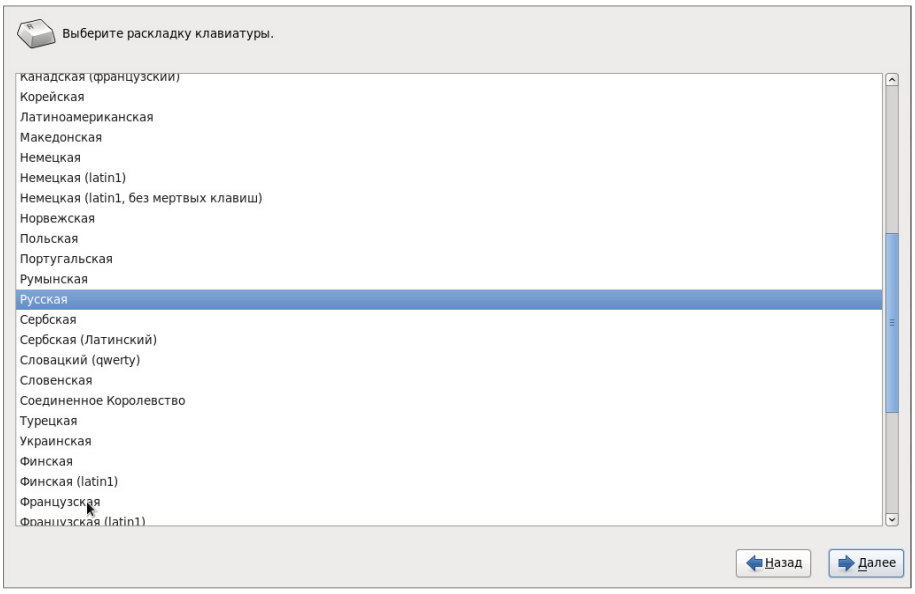


Рисунок 11 – Выбор раскладки клавиатуры

12. Затем потребуется выбрать тип устройств, которые будут использоваться при установке. После выбора типа устройств следует нажать кнопку «Далее».

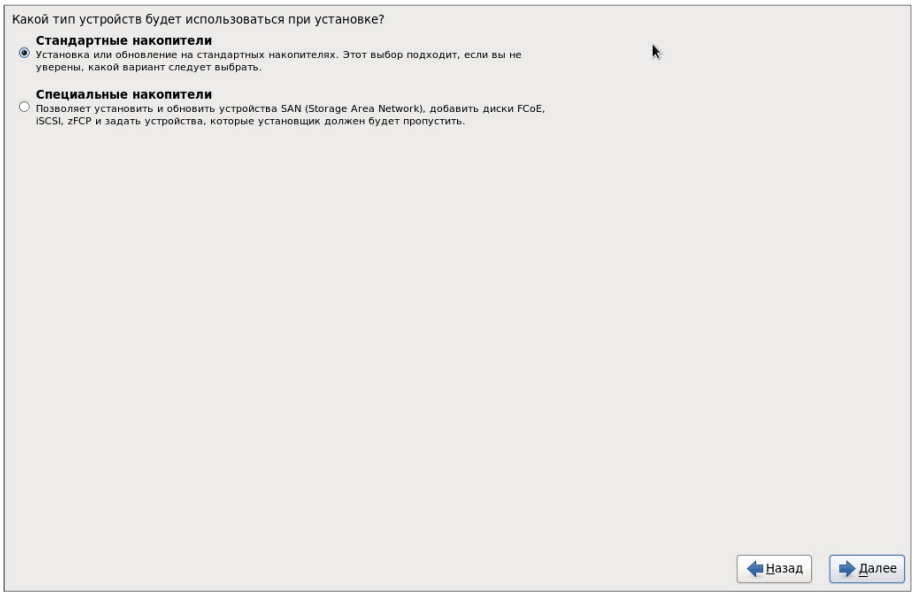


Рисунок 12 – Выбор типа устройств, которые будут использоваться при установке

13. На экране появится окно-предупреждение. Нажмите кнопку «Да, удалить данные» - если устройство хранения не содержит важные данные, кнопку «Нет, сохранить данные» - если устройство хранения содержит важные данные, которые необходимо сохранить.

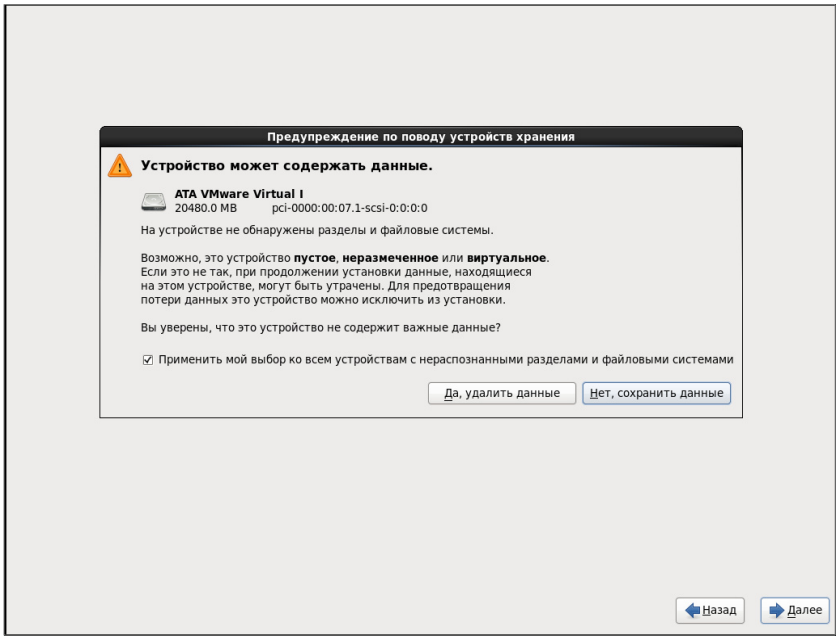


Рисунок 13 – Окно-предупреждение

14. Теперь задайте имя компьютера для его идентификации в сети. Для настройки сети нажмите кнопку «Настроить сеть», для продолжения процесса установки нажмите кнопку «Далее».

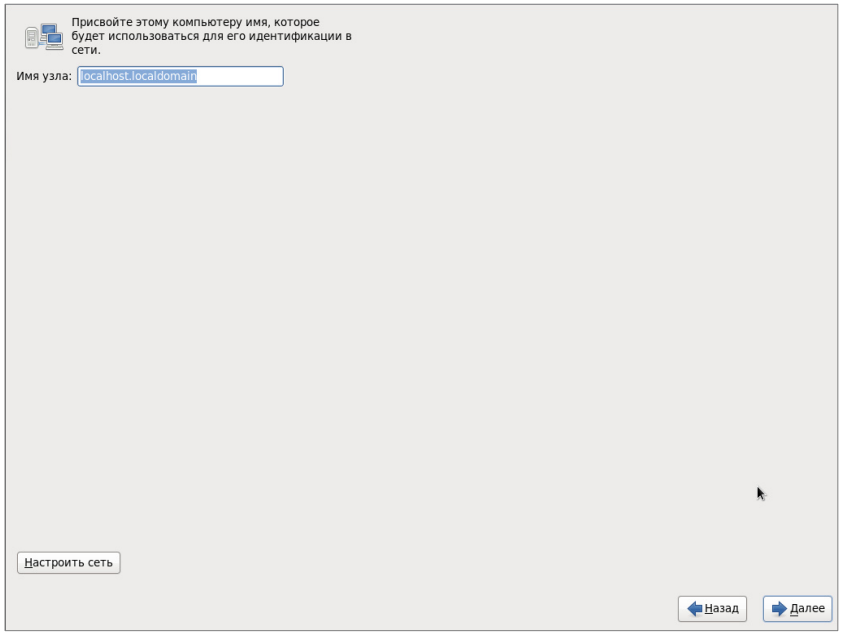


Рисунок 14 – Имя компьютера

15. Задайте настройки сети. Для добавления сетевых соединений нажмите кнопку «Добавить».

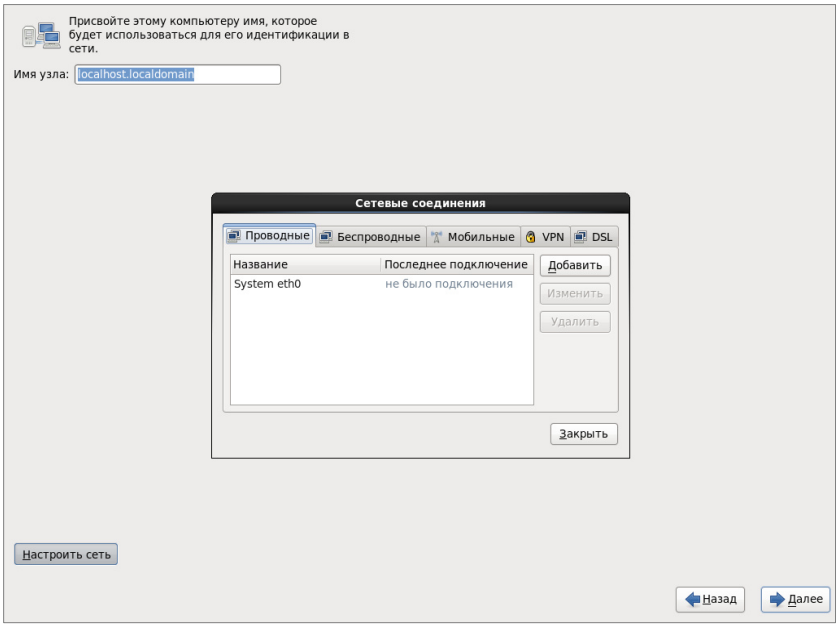


Рисунок 15 – Настройка сети

16. Укажите временную зону, в которой расположен ваш компьютер. Выберите временную зону из списка или на карте, после чего нажмите «Далее».

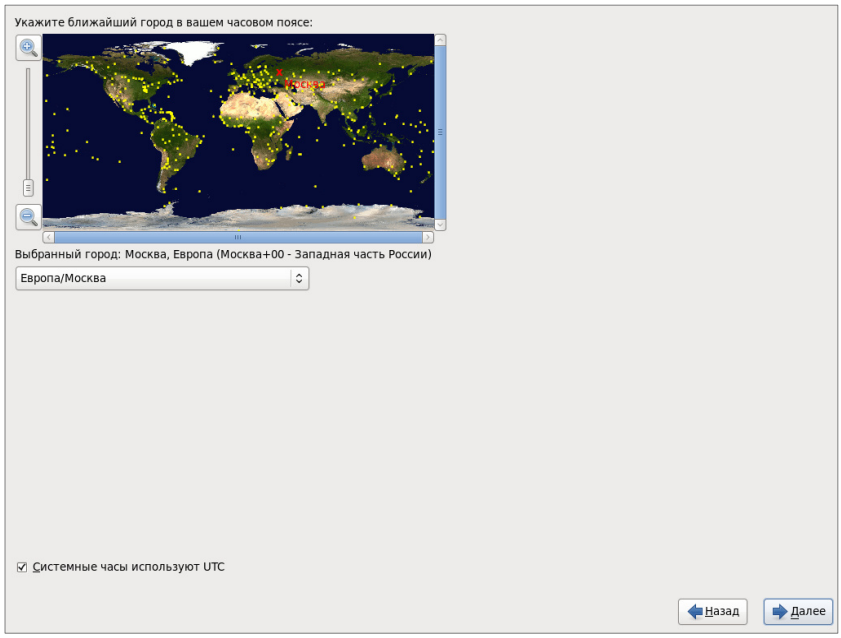


Рисунок 16 – Выбор временной зоны

17. Задайте пароль администратора - суперпользователя с логином root. Пароль не может быть короче 6-ти символов. Для повышения уровня безопасности рекомендуется использовать более длинные и стойкие пароли, представляющие собой по возможности неочевидные сочетания букв, цифр и знаков препинания.

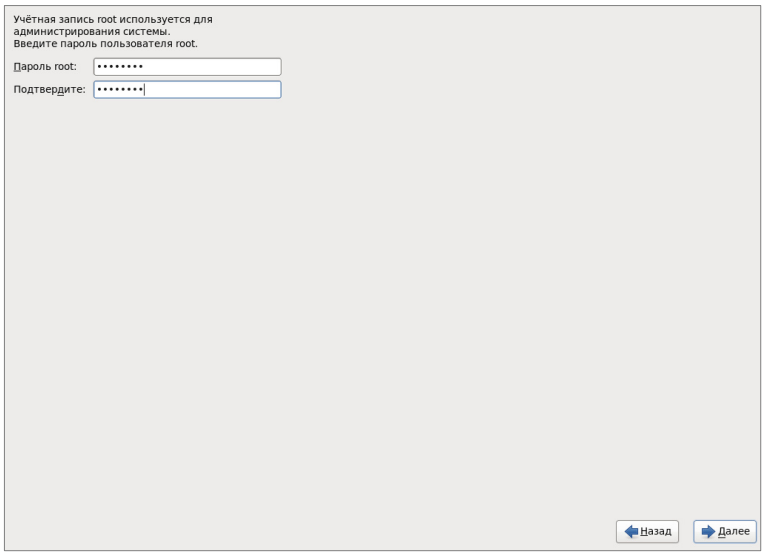


Рисунок 17 – Пароль администратора

Изм.	Лист	№ докум	Подп	Дата

18. На следующем шаге система предложит выбрать тип установки. Выбрав тип установки, нажмите кнопку «Далее».

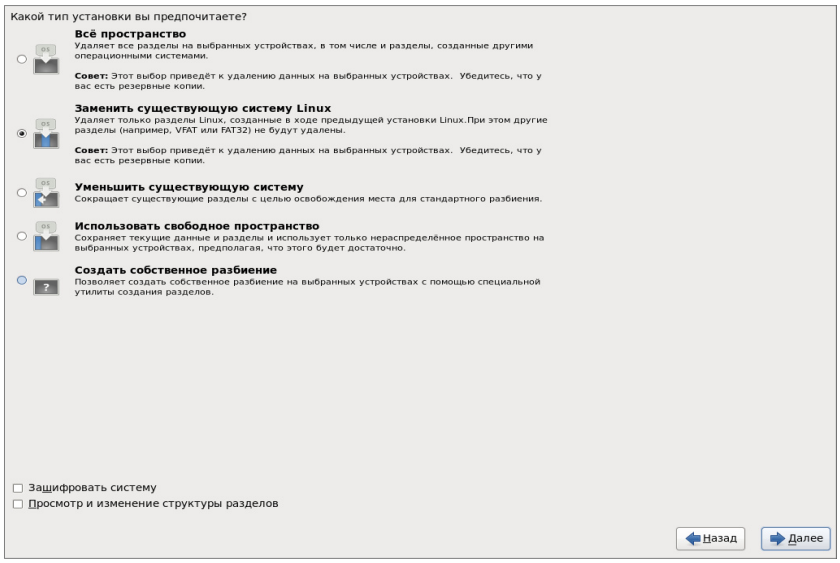


Рисунок 18 – Выбор типа установки

19. Появится предупреждение о выполнении записи информации о хранилище на диск. Если вы уверены, что этот диск действительно неразмеченный, нажмите «Сохранить изменения на диск».

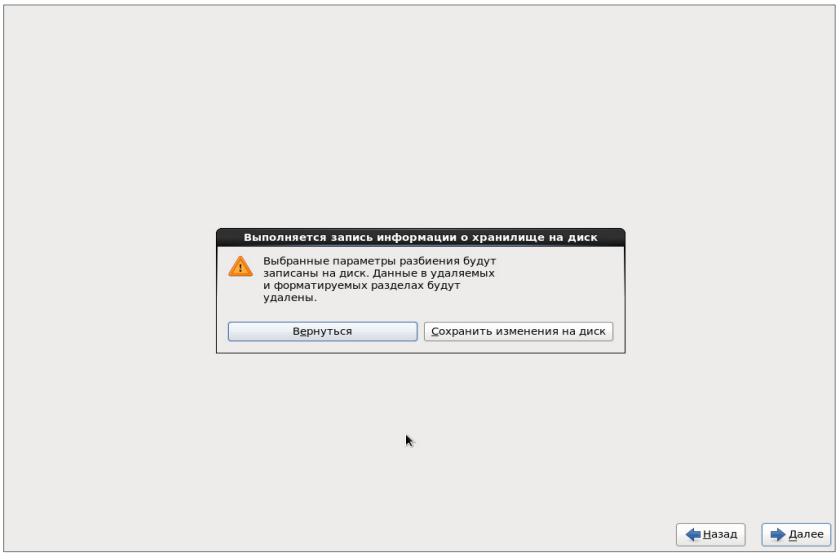


Рисунок 19 – Окно-предупреждение

20. Затем система предложит выбрать для установки нужные программы с указанием требуемых пакетов. Для обеспечения информационной безопасности необходимо установить все реализующие функции защиты информации программные пакеты, перечисленные в

Приложении к настоящему руководству. Это можно сделать на данном шаге, выбрав так называемую полную установку, т.е. в ручном режиме, используя кнопку «Дополнительные пакеты», выбрать все программы и все пакеты, или позже, проведя так называемую выборочную доустановку, аналогично тому, как это описано в подразделе 10.3 для пакета утилиты AIDE, причем при задании команды yum install можно указывать не один, а сразу несколько или все пакеты, перечисленные в Приложении.

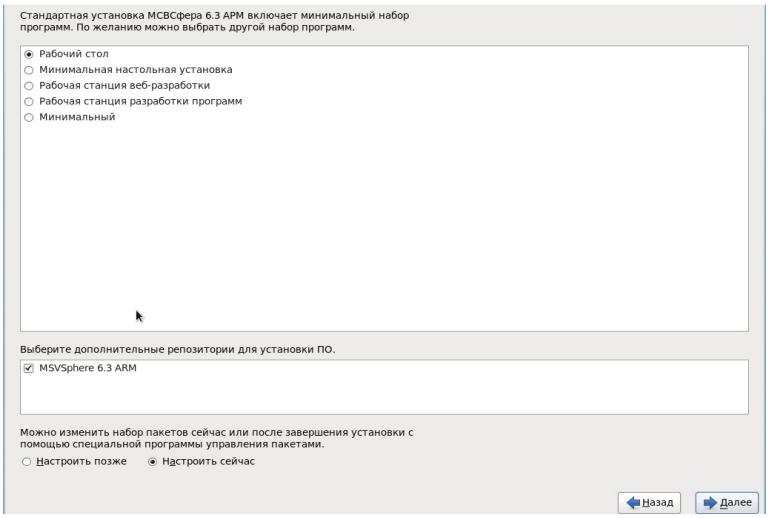


Рисунок 20 – Выбор наборов программ

21. Пример окна выбора программ и дополнительных пакетов для установки.

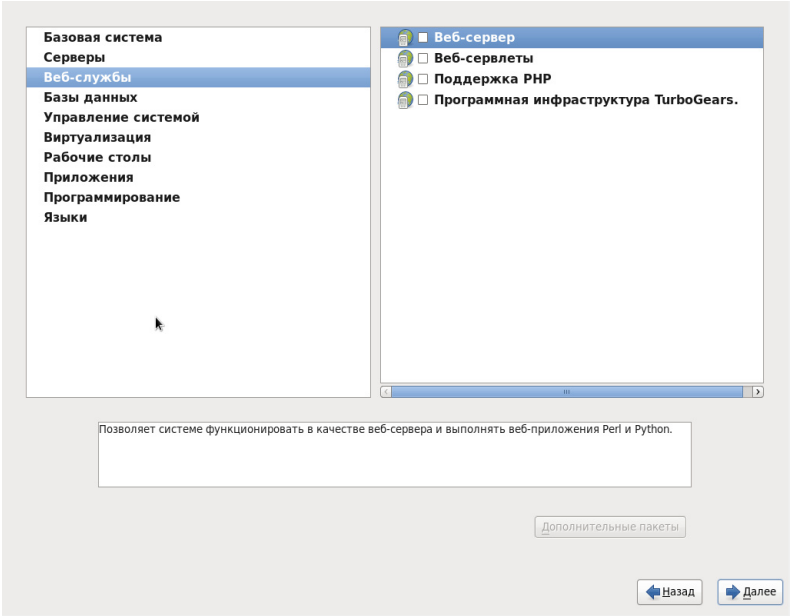


Рисунок 21 – Выбор программ и дополнительных пакетов

Изм.	Лист	№ докум	Подп	Дата

22. Система в автоматическом режиме произведет все необходимые проверки и выполнит установку программного обеспечения. Время установки зависит от скорости работы жестких дисков вашего компьютера.

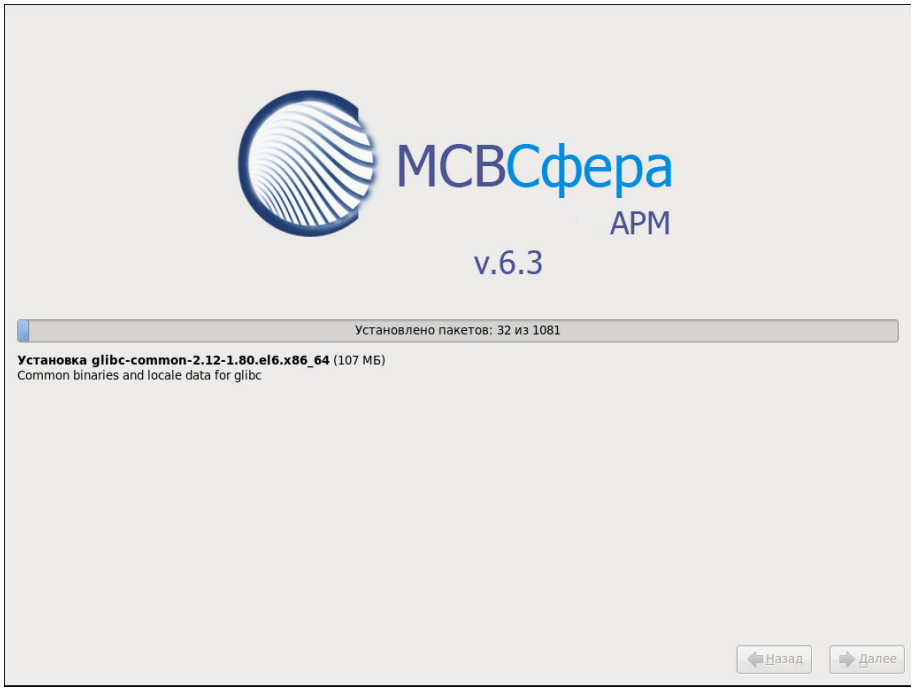


Рисунок 22 – Установка программного обеспечения

23. По завершении установки появится соответствующее сообщение. Извлеките диск, с которого производилась установка, и нажмите кнопку «Перезагрузка».

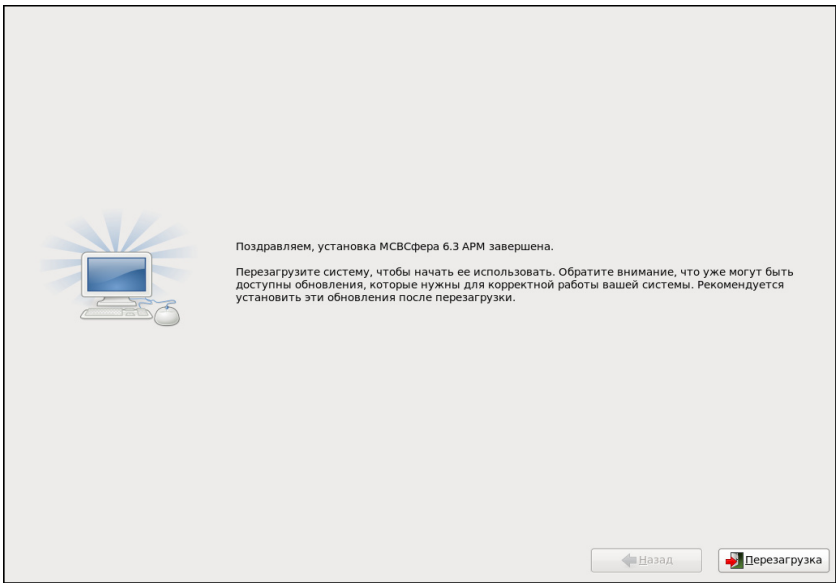


Рисунок 23 – Экран после установки

Изм.	Лист	№ докум	Подп	Дата

24. После перезагрузки появится приветствие. Нажмите кнопку «Вперед».

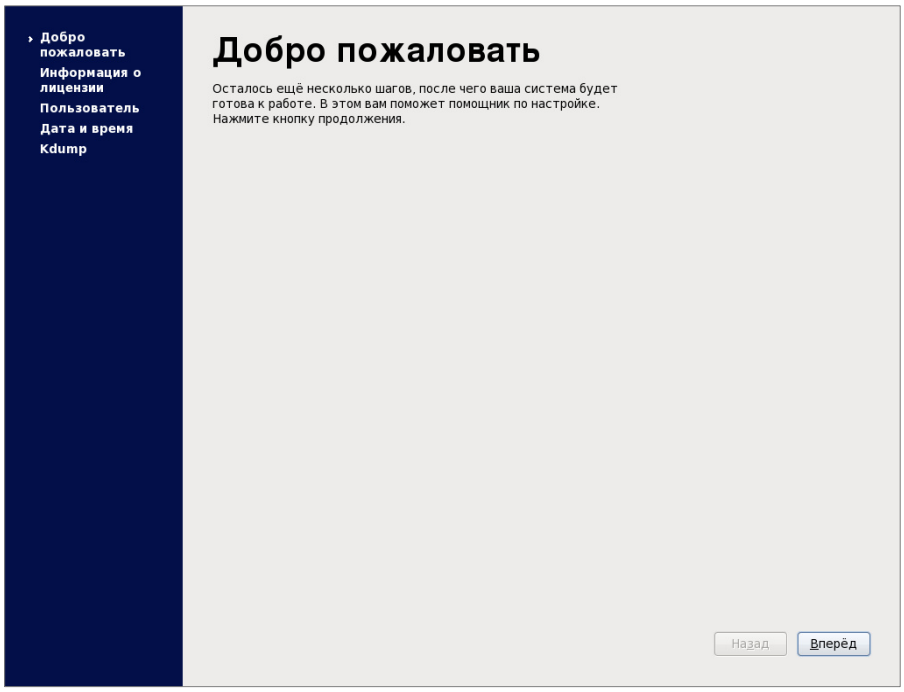


Рисунок 24 – Программа первоначальной настройки ситемы

25. Система предложит принять условия лицензионного соглашения.

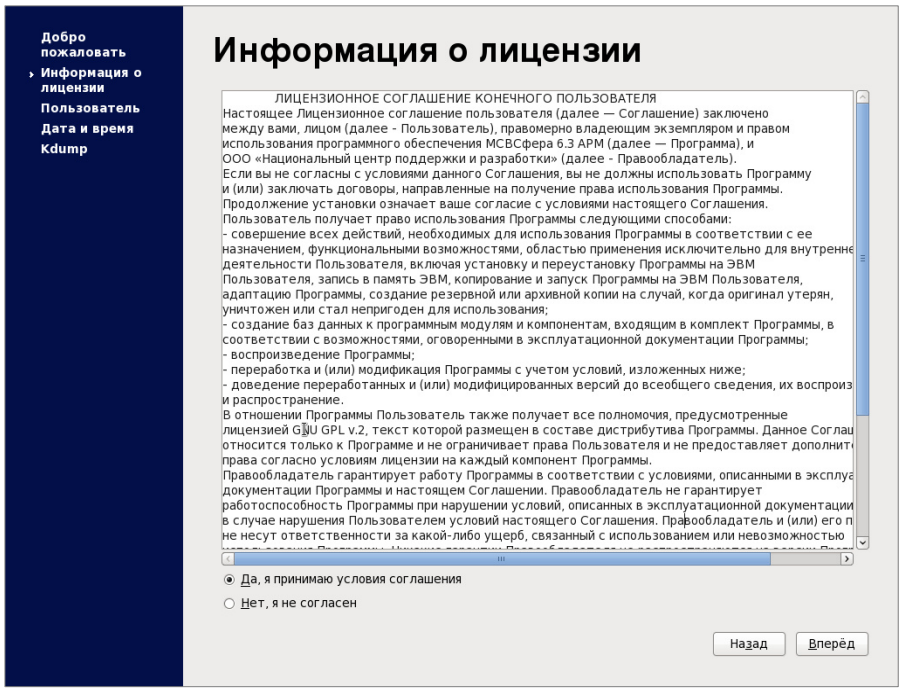


Рисунок 25 – Лицензионное соглашение

26. Теперь можно создать пользователя, не обладающего полномочиями администратора. Задайте краткое «Имя пользователя», которое будет использоваться в качестве системного логина, «Полное имя» в удобном для понимания виде и пароль. Затем нажмите кнопку «Вперед».

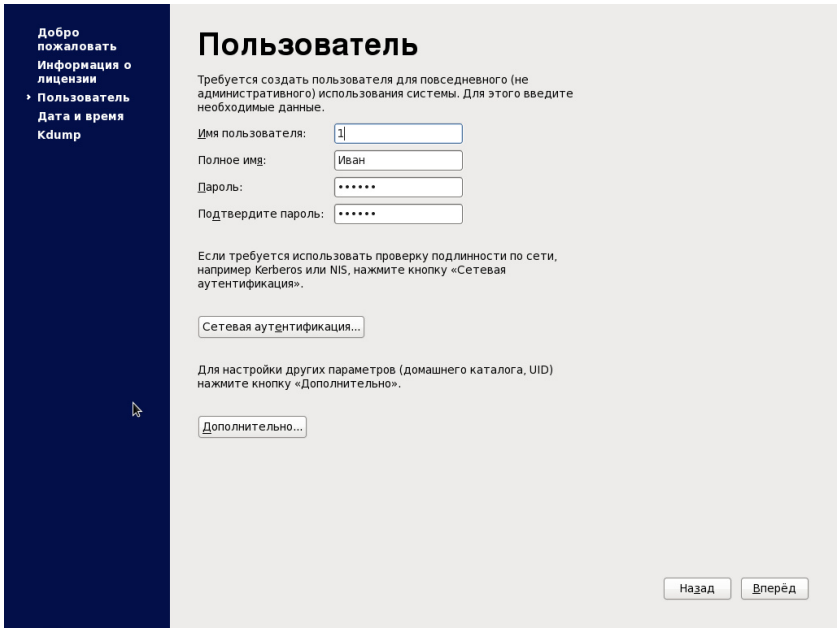


Рисунок 26 – Создание пользователя для повседневной работы

27. После этого можно установить системную дату и время. Введите их значения и нажмите кнопку «Вперед».

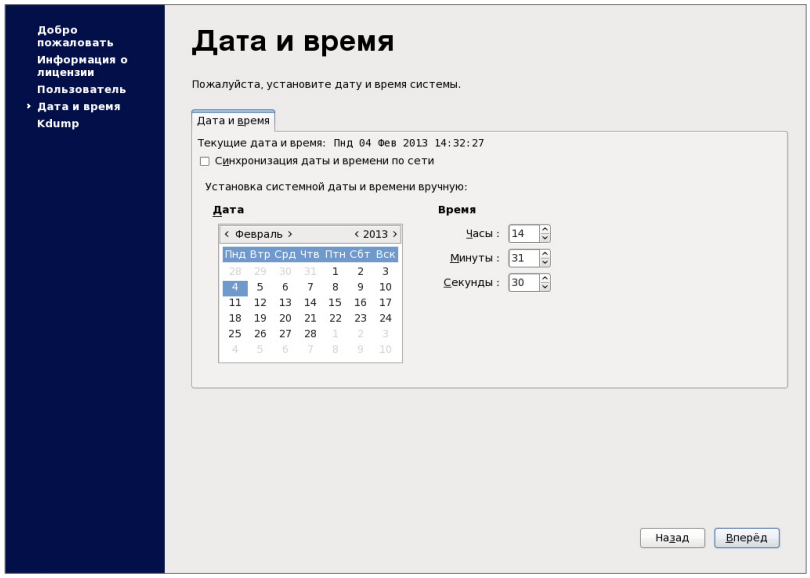


Рисунок 27 – Задание системной даты и времени

Изм.	Лист	№ докум	Подп	Дата

28. Система предложит выполнить настройку механизма сбора информации о системных сбоях Kdump. Задайте необходимые значения и нажмите «Готово».

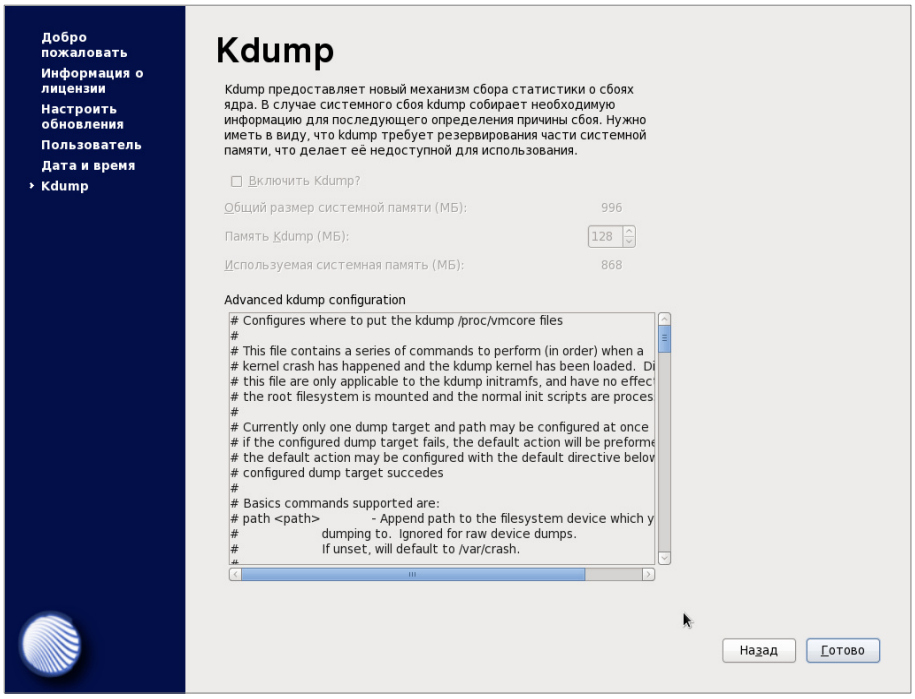


Рисунок 28 – Настройка системы сбора информации о системных сбоях Kdump

29. Выберите из списка пользователя.

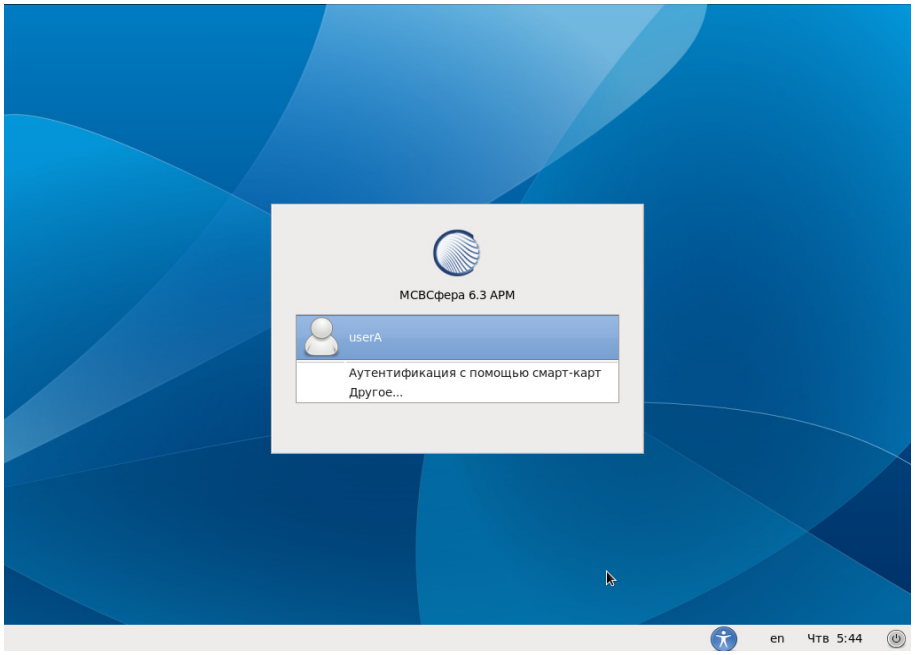


Рисунок 29 – Выбор пользователя

Изм.	Лист	№ докум	Подп	Дата

30. На экране появится рабочий стол следующего вида:

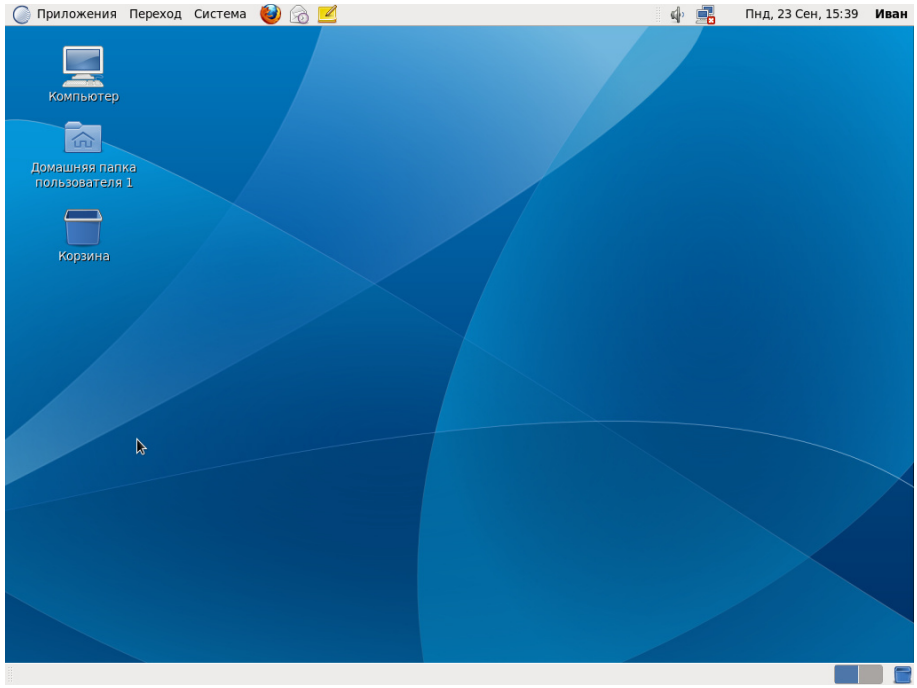


Рисунок 30 – Рабочий стол после завершения установки

2.2 Обновление системы

Обновление системы выполняется с использованием команды yum или при помощи приложения «Обновление программ».

Обновление с компакт-диска с использованием команды yum выполняется следующим образом:

1. В устройство чтения оптических дисков установить компакт-диск с набором обновлений, который должен иметь метку тома «MSVSphere_6.3_ARM_Updates» и каталог updates с репозиторием обновлений.
2. В конфигурационном файле /etc/yum.repos.d/updates_ex.repo установить значение параметра enabled равным 1.
3. Выполнить команду yum update из командной строки.

Для обновления с помощью приложения «Обновление программ» выберите Система → Администрирование → Обновление программ (рис. 31).

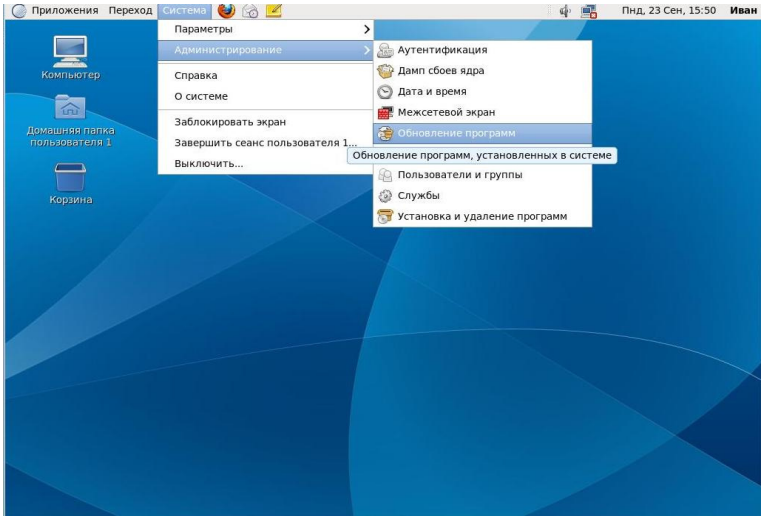


Рисунок 31 - Запуск приложения

Если обновления есть - нажмите “Установить обновления”, в данном случае обновлений нет (рис. 32).

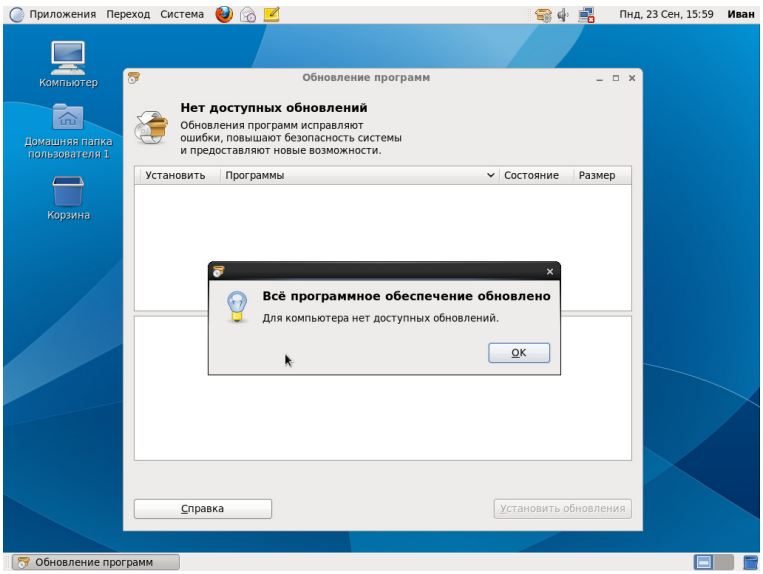


Рисунок 32– Обновление программ

Для обновления через Internet в конфигурационном файле необходимо указать адрес репозитория обновлений, затем выполнить команду yum update или запустить графическое приложение «Обновление программ», как показано на рис. 31 и рис. 32.

3 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

3.1 Основные сведения

Средства идентификации и аутентификации МСВСфера 6.3 АРМ предоставляют следующие возможности:

- идентификация и аутентификация пользователей;
- идентификация и аутентификация устройств;
- управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;
- управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации;
- защита обратной связи при вводе аутентификационной информации;
- идентификация и аутентификация сетевого входа;
- идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа.

Вышеперечисленные возможности управления доступом реализуются с помощью следующих программных компонент:

- приложение "Конфигурация аутентификации";
- приложение "Kerberos Authentication Configuration";
- приложение "Менеджер пользователей";
- утилиты chage, useradd, usermod.

3.2 Приложение "Конфигурация аутентификации"

Для настройки механизмов идентификации и аутентификации пользователей предназначено приложение «Конфигурация аутентификации», которое может быть запущено из меню «Система–>Администрирование–>Аутентификация» и доступно только в режиме администратора. Во вкладке «Идентификация и аутентификация» данного приложения нужно

выбрать, как должна выполняться аутентификация пользователей. Возможны следующие варианты:

- локальная аутентификация. При данном виде аутентификации используются только локальные учётные записи пользователей;
- аутентификация с использованием протокола LDAP. При данном виде аутентификации используется информация о пользователях, расположенная на указанном сервере LDAP;
- аутентификация с использованием системы IPA v2. Аутентификация выполняется через указанный IPA-сервер;
- аутентификация с использованием системы NIS. Аутентификация выполняется через указанный NIS-сервер;
- аутентификация с использованием системы Microsoft Active Directory. Для подключения к домену Active Directory используется система Samba Winbind.

Окно приложения «Конфигурация аутентификации», в котором задана локальная аутентификация, приведено на рис. 33.

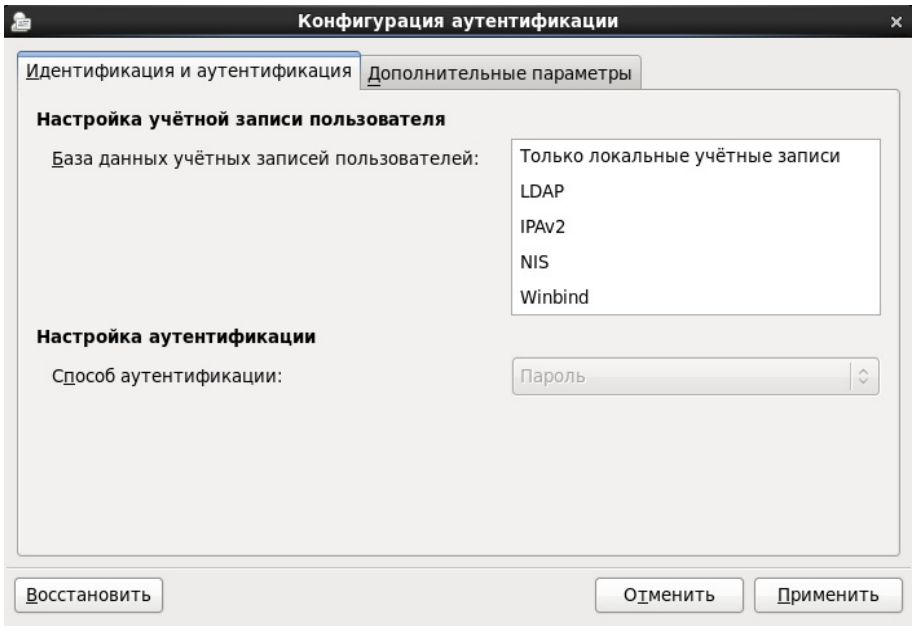


Рисунок 33 - Окно приложения "Конфигурация аутентификации" вкладка "Идентификация и аутентификация"

При настройке аутентификации на виртуальной машине с использованием протокола LDAP необходимо указать базовое DN для поиска LDAP и сервер LDAP. Если планируется

использовать TLS для шифрования соединений, то необходимо установить галочку рядом с соответствующей надписью и загрузить сертификат. В качестве способа аутентификации можно выбрать пароль LDAP или пароль Kerberos. Окно настройки аутентификации с использованием протокола LDAP приведено на рис. 34.

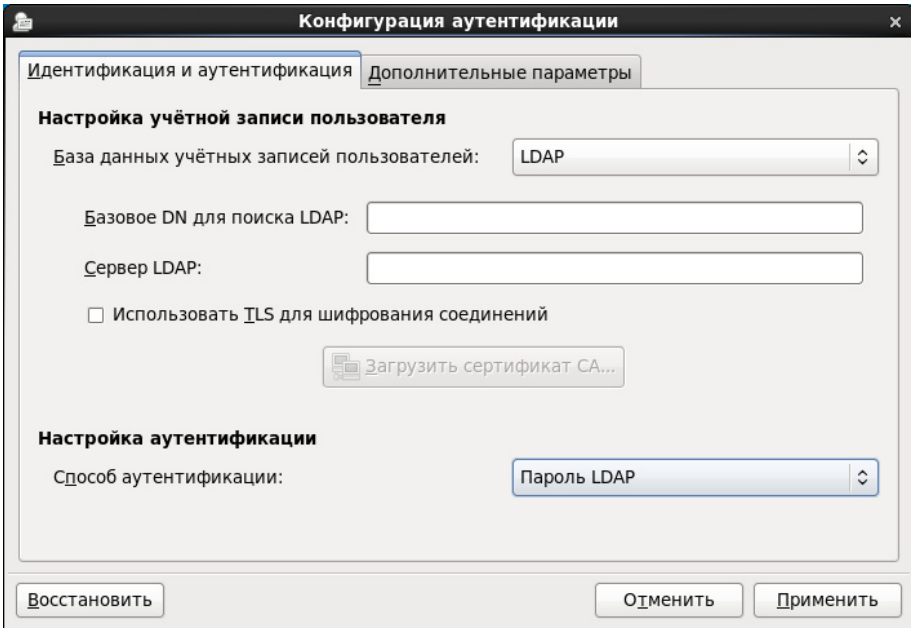


Рисунок 34 - Окно настройки аутентификации с использованием протокола LDAP

На рис. 35 приведено окно настройки аутентификации с использованием системы IPA v2. При настройке аутентификации с использованием IPAv2 задаётся домен IPA, область IPA и сервер IPA. По умолчанию выполняется настройка протокола NTP, но ее можно отключить.

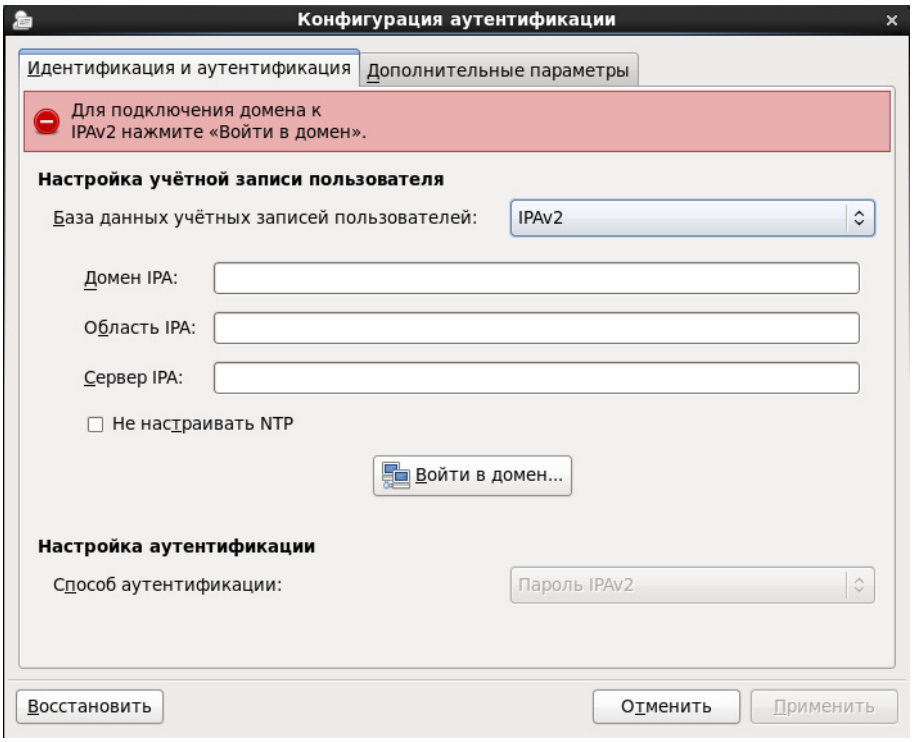


Рисунок 35 - Окно настройки аутентификации с использованием системы IPA v2

Окно настройки аутентификации с использованием системы NIS приведено на рис. 36. При настройке аутентификации с использованием системы NIS задаётся домен и сервер NIS. В качестве способа аутентификации можно выбрать пароль NIS или пароль Kerberos.

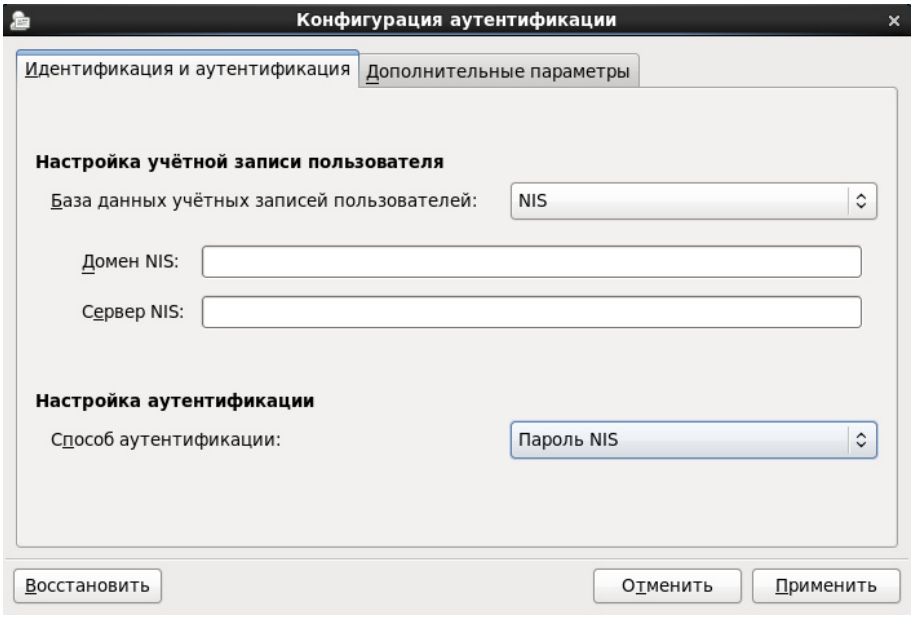


Рисунок 36 - Окно настройки аутентификации с использованием системы NIS

На рис. 37 приведено окно настройки аутентификации с использованием системы Winbind. При настройке аутентификации с использованием системы Winbind задаётся домен Windows, к которому необходимо подключиться, модель защиты, область Active Directory, к которой будет подключаться Samba-сервер; указываются контроллеры домена и оболочка для настройки учётной записи пользователя Windows. Установка флага «Разрешить автономный вход» позволяет сохранять аутентификационную информацию в локальном кэше.

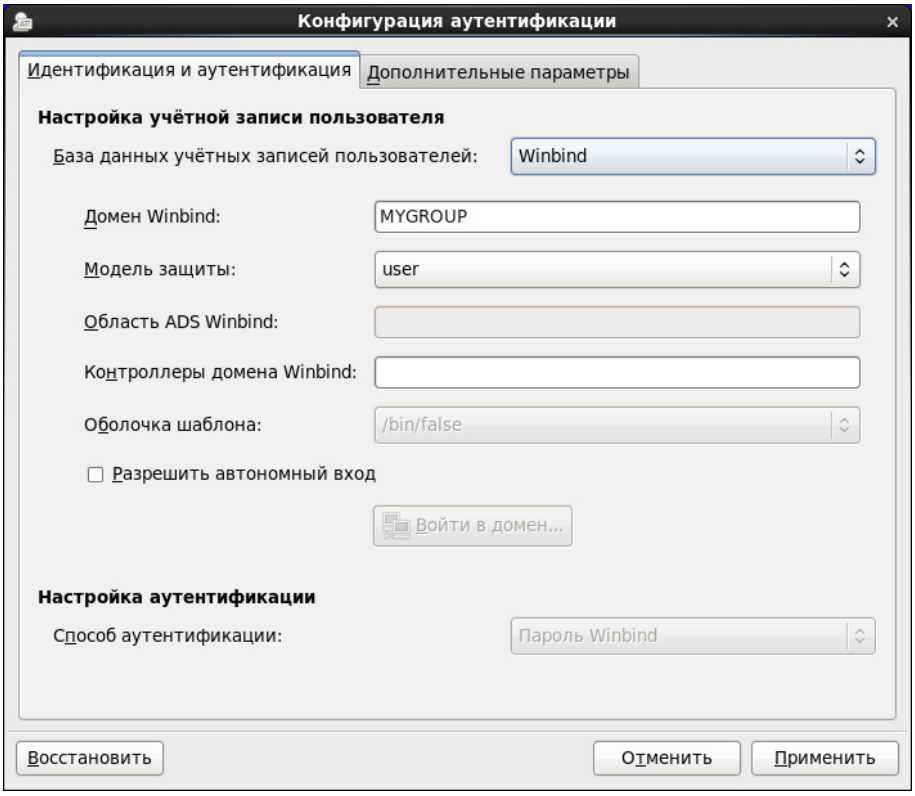


Рисунок 37 - Окно настройки аутентификации с использованием системы Winbind

Вкладка «Дополнительные параметры» приложения «Конфигурация аутентификации» позволяет управлять следующими опциями аутентификации (рис. 38):

- поддержкой чтения отпечатков пользователя (при наличии соответствующего оборудования);
- локальным управлением доступом (через файл /etc/security/access.conf);
- выбором алгоритма хэширования паролей;
- созданием домашнего каталога при первом входе пользователя в систему, что удобно при централизованном управлении учётными записями пользователей, например, через LDAP;

– поддержкой аутентификации с использованием смарт-карт (при наличии соответствующего оборудования).

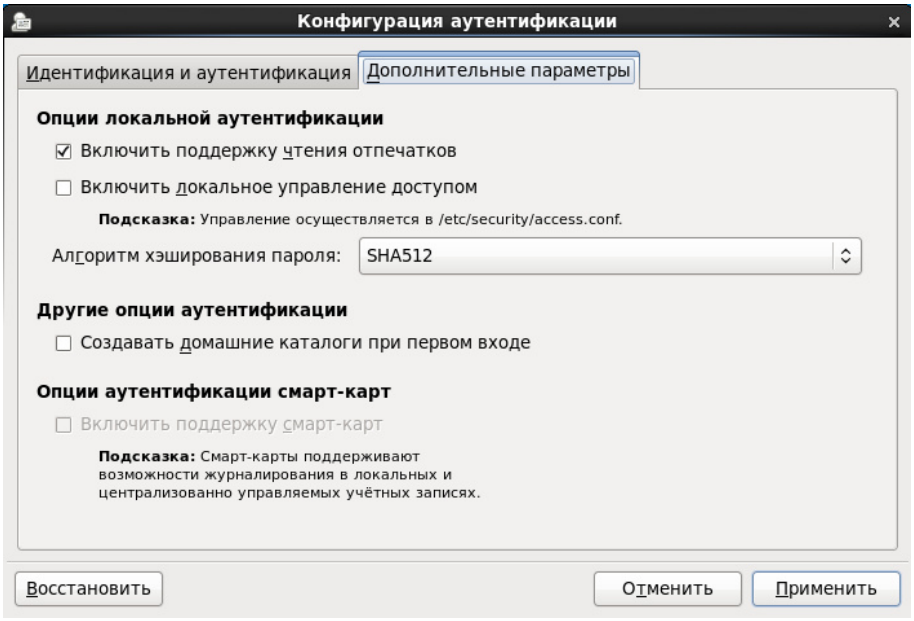


Рисунок 38 - Вкладка «Дополнительные параметры» приложения «Конфигурация аутентификации»

По умолчанию система обеспечивает защиту пароля пользователя при входе, например, обеспечивает защиту обратной связи при вводе аутентификационной информации – скрытую обратную связь.

3.3 Приложение "Kerberos Authentication Configuration"

Для настройки механизмов идентификации и аутентификации сетевых пользователей предназначено приложение «Kerberos Authentication Configuration», которое запускается из меню «Система–>Параметры–>Network Authentication».

Kerberos это сетевой протокол аутентификации, позволяющий передавать данные через незащищённые сети для безопасной идентификации и обеспечивающий взаимную аутентификацию (оба пользователя через сервер подтверждают личности друг друга).

На вкладке "Kerberos" (рис. 39) выполняется настройка Kerberos пользователей и билетов (временные данные, выдаваемые клиенту для аутентификации на сервере, на котором располагается необходимая служба).

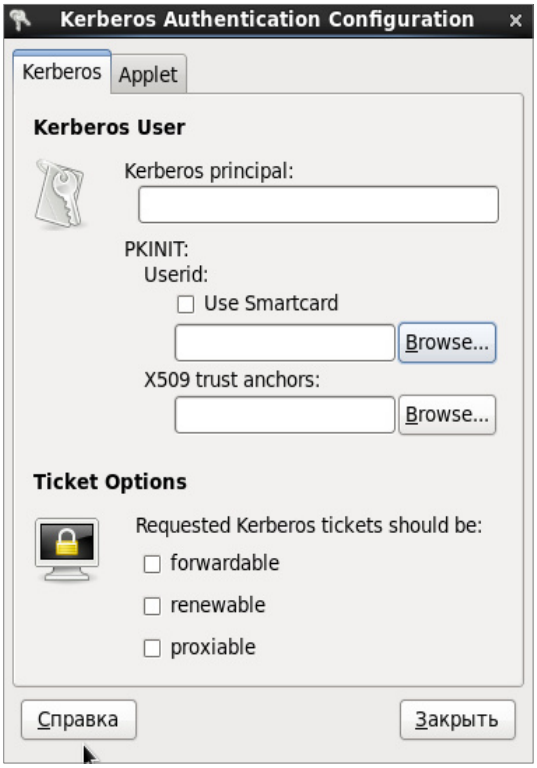


Рисунок 39 - Вкладка "Kerberos"
приложения «Kerberos Authentication Configuration»

В поле Kerberos principal указывается принципал пользователя - уникальное имя для клиента, для которого разрешается аутентификация в Kerberos. Для того чтобы использовать текущее имя пользователя, нужно оставить поле пустым. Если изменить эту настройку, необходимо будет уничтожить кэш учетных данных, прежде чем эти параметры вступят в силу.

Помимо пользовательских принципалов в базе данных Kerberos должны существовать специальные служебные принципалы для каждой работающей службы. Например, если ldap.example.com предоставляет службу LDAP, вам нужен служебный принципал, ldap/ldap.example.com@EXAMPLE.COM, для аутентификации этой службы перед всеми клиентами.

Соглашение именования для служебных принципалов: *служба/имяхоста@ОБЛАСТЬ*, где имя_хоста - полное имя хоста. Действительные дескрипторы служб приведены в табл. 1.

Таблица 1. Действительные дескрипторы служб

Дескриптор службы	Служба
host	Telnet, RSH, SSH
nfs	NFSv4 (с поддержкой Kerberos)
HTTP	HTTP (с аутентификацией Kerberos)
imap	IMAP
pop	POP3
ldap	LDAP

Служебные принципалы сходны с пользовательскими, но имеют существенные отличия. Основное отличие между ними заключается в том, что ключ пользовательского принципала защищен паролем - когда пользователь получает билет на предоставление билета от KDC, ему нужно ввести свой пароль для того, чтобы Kerberos смог расшифровать этот билет. Ключ для расшифровки первого билета служебного принципала получается администратором от KDC всего один раз и хранится в локальном файле с именем *keytab*. Службы, такие как демон SSH, читают этот ключ и, при необходимости, используют его для получения нового билета автоматически. Файл keytab по умолчанию находится в /etc/krb5.keytab.

Расширение PKINIT предоставляет возможность использовать ассиметричные криптографические алгоритмы, возможность интерактивной регистрации пользователя с помощью микропроцессорных карточек (рис. 40).

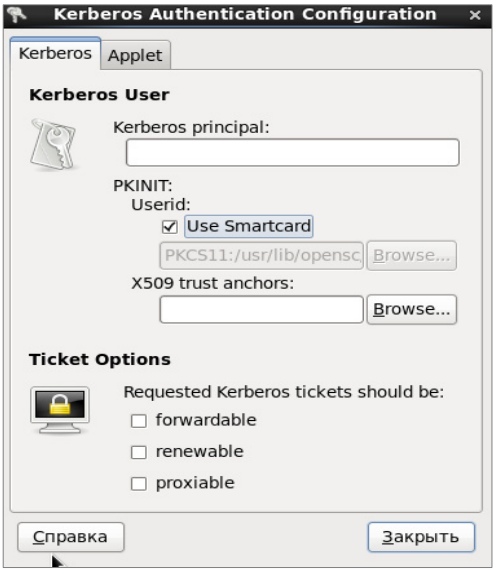


Рисунок 40 - Использование смарт-карт для аутентификации

PKINIT позволяет реализовать двухфакторную аутентификацию пользователя на этапе предаутентификации протокола Kerberos – пользователь должен иметь смарт-карту с хранящимися в памяти карты сертификатом и закрытым ключом и знать ее PIN-код, чтобы иметь возможность использовать закрытый ключ для формирования цифровой подписи. Использование смарт-карт и цифровых сертификатов стандарта X.509 позволяет усилить функции безопасности операционной системы.

Установить тип запрашиваемого Kerberos билета можно, выбрав соответствующий параметр:

forwardable - означает, что запрошенный билет Kerberos должен быть переслан, изменение этого параметра требует от вас, чтобы заново была пройдена аутентификация (левой кнопкой мыши щелкнуть на иконке в трее и ввести пароль);

renewardable - означает, что запрошенный билет Kerberos должен быть возобновлен, изменение этого параметра требует от вас, чтобы заново была пройдена аутентификация (левой кнопкой мыши щелкнуть на иконке в трее и ввести пароль);

proxiable - передает новый билет Kerberos серверу в качестве доверенности, изменение этого параметра требует от вас, чтобы заново была пройдена аутентификация (левой кнопкой мыши щелкнуть на иконке в трее и ввести пароль).

На вкладке "Applet" настраиваются: число минут до истечения срока использования учетных данных (появляется уведомление) и отображение иконки в трее (отключение иконки в трее будет так же отключать уведомления) (рис. 41).

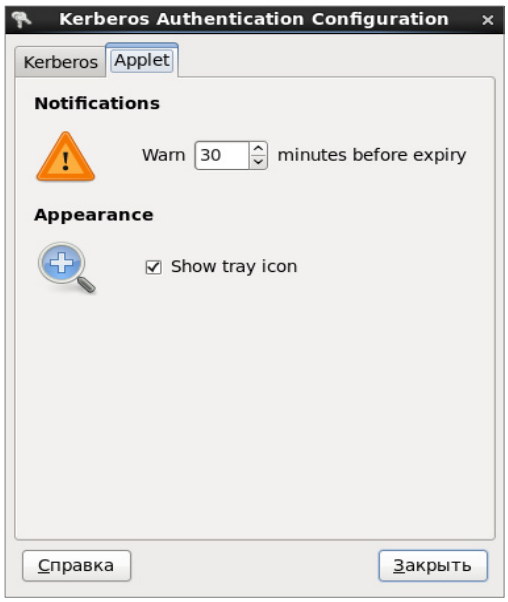


Рисунок 41 - Вкладка "Applet" приложения «Kerberos Authentication Configuration»

3.4 Приложение "Менеджер пользователей"

В целях безопасности рекомендуется требовать, чтобы пользователи периодически меняли свои пароли. Это можно сделать при редактировании свойств пользователя на вкладке «Сведения о пароле» программы «Менеджер пользователей», которая запускается из меню «Система–>Администрирование–>Пользователи и группы» (рис. 42).

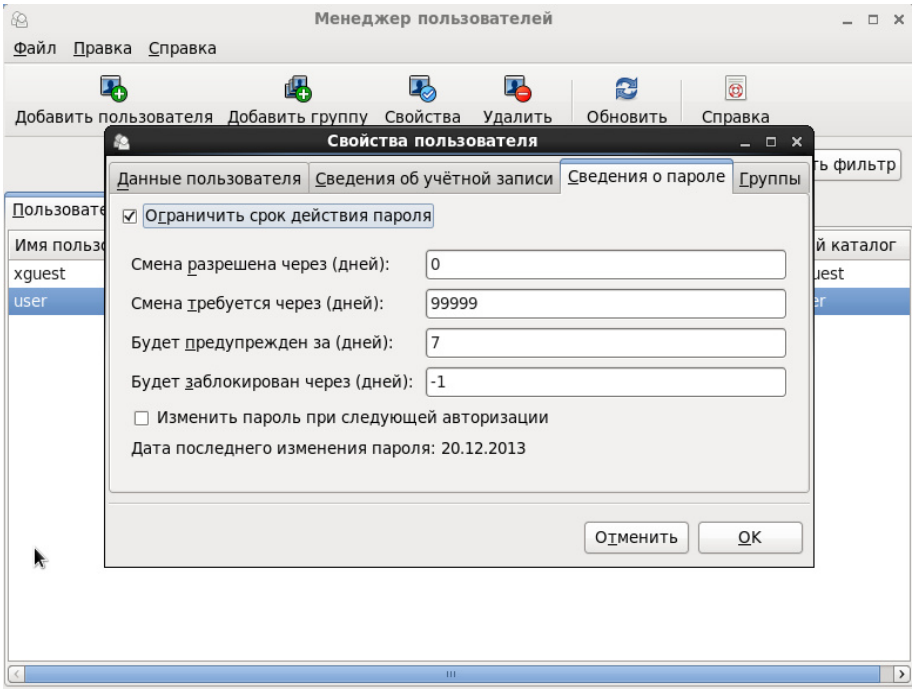


Рисунок 42 - Редактирование пользователя на вкладке "Сведения о пароле"

Для ограничения пароля пользователя нужно выбрать его в списке и нажать кнопку "Свойства", в открывшемся диалоговом окне нужно выбрать вкладку "Сведения о пароле" и отметить галочкой пункт "Ограничить срок действия пароля". После этого необходимо задать количество дней, после которых будет разрешена смена пароля, количество дней, после которых потребуется смена пароля, количество дней, за которые пользователь будет предупрежден о необходимости смены пароля, и количество дней, после которых пароль будет заблокирован. В этом же диалоговом окне указана дата последнего изменения пароля. Для того, чтобы пароль был изменен при следующем входе пользователя, нужно отметить галочкой пункт "Изменить пароль при следующей авторизации".

Для ограничения срока действия учетной записи нужно перейти в том же диалоговом окне на вкладку "Сведения об учетной записи" (рис. 43) и отметить галочкой пункт "Ограничить срок действия учетной записи", указав срок истечения учетной записи, или пункт "Локальный пароль заблокирован".

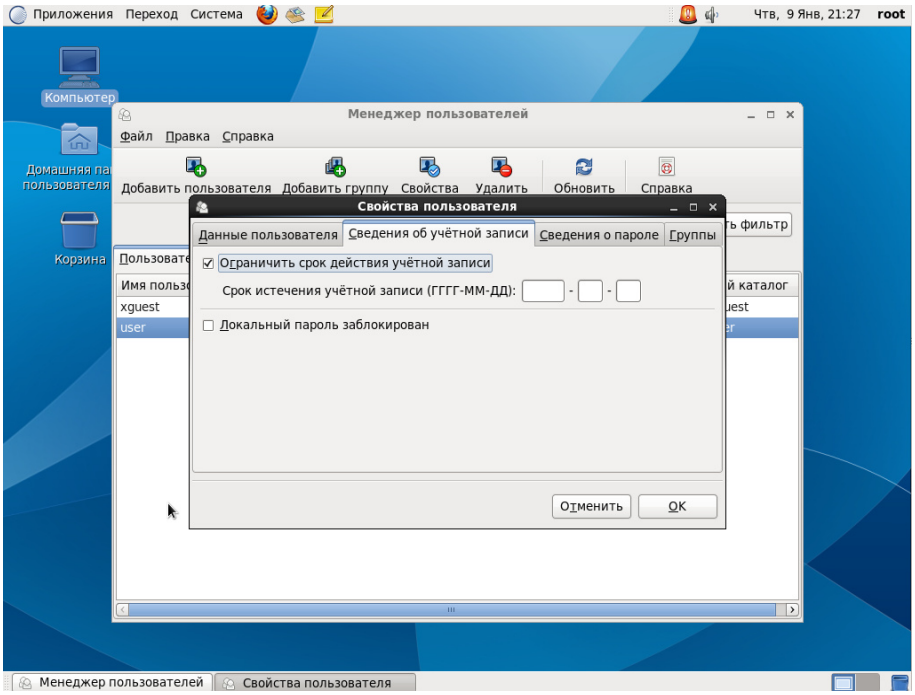


Рисунок 43 - Диалоговое окно "Свойства пользователя"
вкладка "Сведения об учетной записи"

Для формирования и присвоения идентификатора новому пользователю нужно в приложении "Менеджер пользователей" перейти к диалоговому окну "Добавить нового пользователя" (рис. 44), заполнить требуемые поля, отметить галочкой пункт "Указать ID пользователя вручную" и ввести идентификатор. Аналогично можно поступить с идентификатором группы пользователя - пункт "Укажите ID группы вручную".

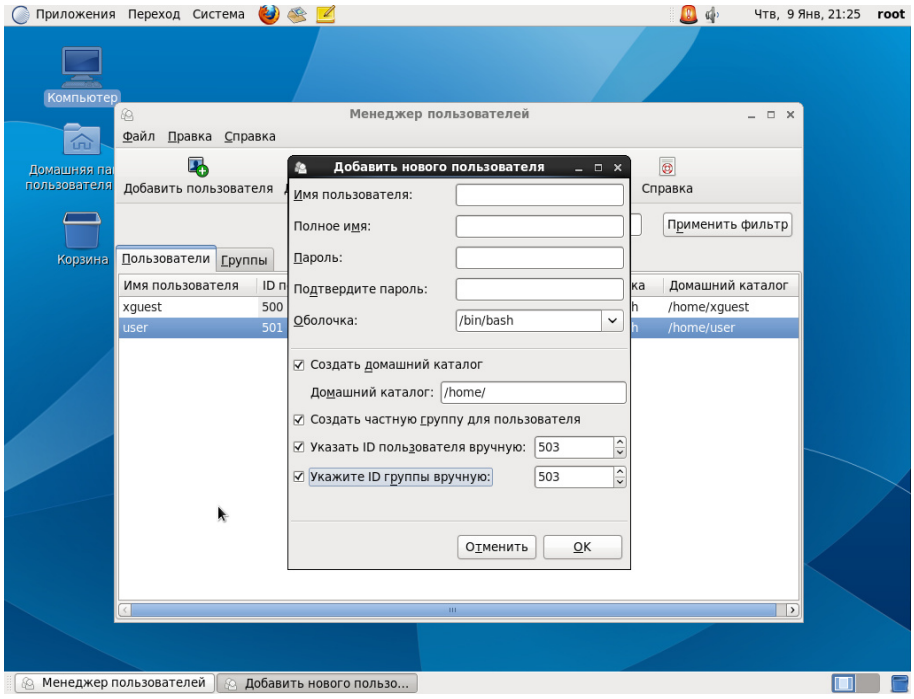


Рисунок 44 - Добавление нового пользователя

Для удаления пользователя и его идентификактора, необходимо выбрать пользователя в списке и нажать кнопку "Удалить". В появившемся окне (рис. 45) согласиться с полным удалением пользователя и информации о нем.

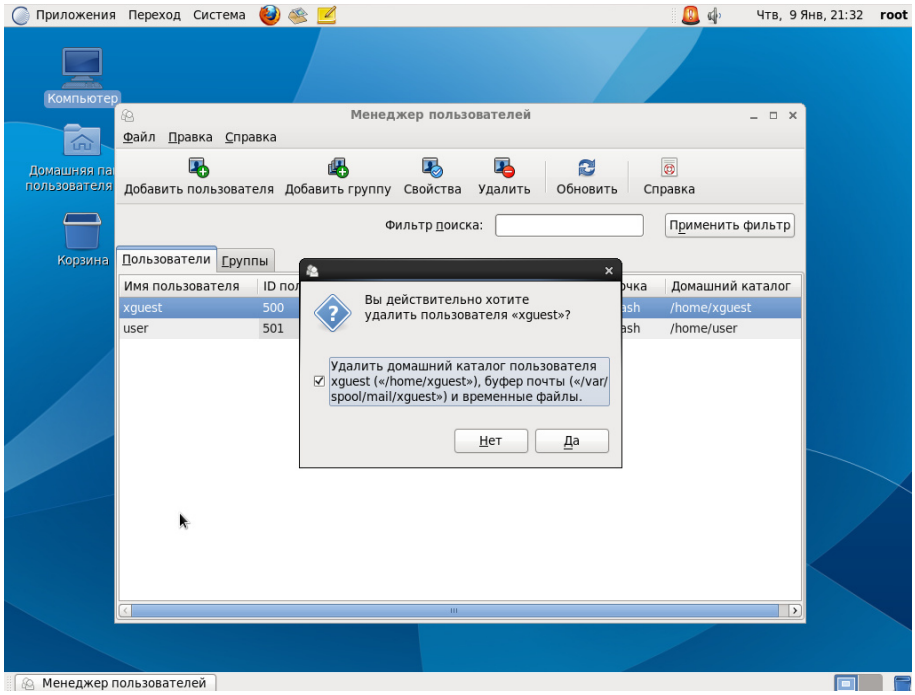


Рисунок 45 - Удаление пользователя

Изм.	Лист	№ докум	Подп	Дата

3.5 Утилита chage

Чтобы настроить принудительную смену пароля пользователя в командной строке, необходимо воспользоваться командой chage.

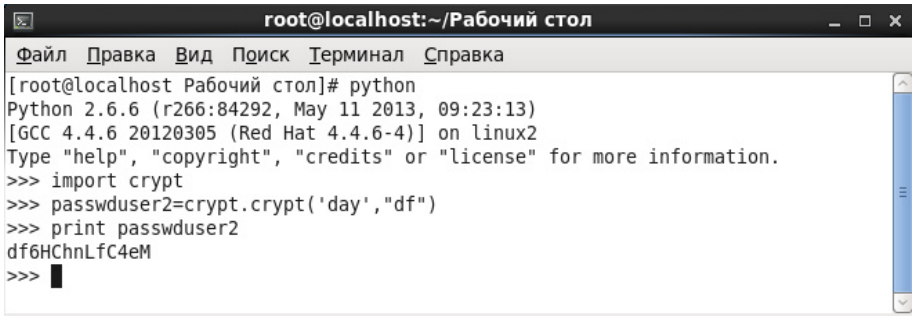
Если системный администратор хочет, чтобы пользователь задал пароль при первом входе в систему, он может назначить пустой или какой-то исходный пароль, который истечет немедленно, и, таким образом, пользователь должен будет сменить его при первом входе.

Для принудительной смены пароля при первом входе пользователя необходимо выполнить следующие действия:

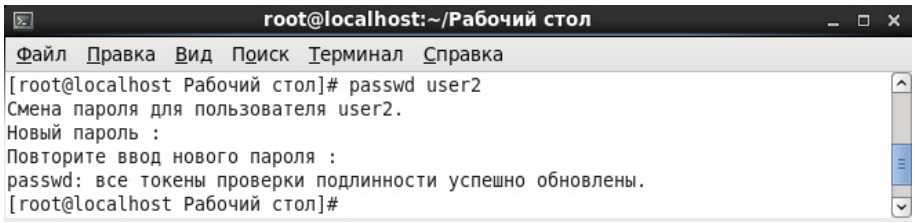
1. заблокировать пароль пользователя с помощью команды usermod –L <имя пользователя>
2. для немедленной смены пароля использовать команду chage –d 0 <имя пользователя>
3. разблокировать учетную запись, назначив начальный пароль.

Назначить начальный пароль можно следующими способами:

1. назначить пустой пароль с помощью команды usermod –p "" <имя пользователя>
2. запустить интерпретатор командной строки Python с помощью команды python. Выполнить команды, как показано ниже, где в строке passwduser2=crypt.crypt('day',"df"): passwduser2 - название конструкции формирования кодированного пароля, "day" - пароль шифрования, а "df" - комбинация двух больших или маленьких букв, цифр, символов точка (.) или косая черта slash (/).



В результате будет получен кодированный пароль, такой как "df6HChnLfC4eM". Для выхода из Python нажмите [Ctrl+D]. После чего измените пароль пользователя командой passwd <имя пользователя>, вставив в поле "Новый пароль :" полученный кодированный пароль.



4 УПРАВЛЕНИЕ ДОСТУПОМ

4.1 Основные сведения

Средства управления доступом МСВСфера 6.3 АРМ предоставляют следующие возможности:

- управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;
- реализация различных методов управления доступом (дискреционный, мандатный, ролевой), типов доступа (чтение, запись, выполнение или иной тип) и правил разграничения доступа;
- управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами;
- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;
- назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;
- ограничение количества неуспешных попыток входа в информационную систему (доступа к информационной системе);
- предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры защиты информации, и о необходимости соблюдения им установленных правил обработки информации;
- оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему;
- блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу;

- разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации;
- поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки;
- реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;
- регламентация и контроль использования в информационной системе технологий беспроводного доступа;
- регламентация и контроль использования в информационной системе мобильных технических средств;
- управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы);
- обеспечение доверенной загрузки средств вычислительной техники.

Вышеперечисленные возможности управления доступом реализуются с помощью следующих программных компонент:

- приложение "Менеджер пользователей";
- списки контроля доступа ACL;
- биты разрешения доступа;
- конфигурационный файл /etc/sudoers;
- приложение "Администрирование SELinux";
- утилиты командной строки;
- библиотеки PAM;
- приложение "Хранитель экрана";
- приложение "Настройка Kickstart";
- конфигурационный файл /boot/grub/grub.conf;
- подсистемы ядра RFKill;
- файл /etc/issue;
- метки безопасности.

4.2 Определение доступа к файлам и папкам

Для задания типа доступа к файлу необходимо щелкнуть правой кнопкой мыши по выбранному файлу и выбрать пункт контекстного меню "Свойства". На вкладке "Права" в блоке "Владелец" указать требуемый тип доступа, например, "Чтение и запись", а в блоке "Остальные" - "Только чтение", как показано на рисунке (рис.45). Администратор root сможет выполнить чтение и запись файла, а остальные пользователи только чтение (рис. 46).

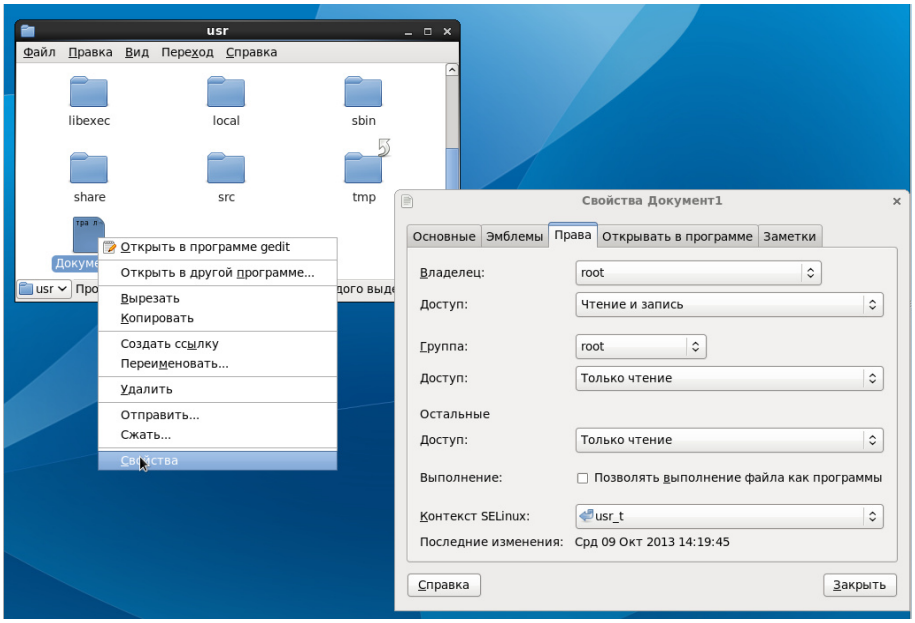


Рисунок 46 - Определение типа доступа для файла

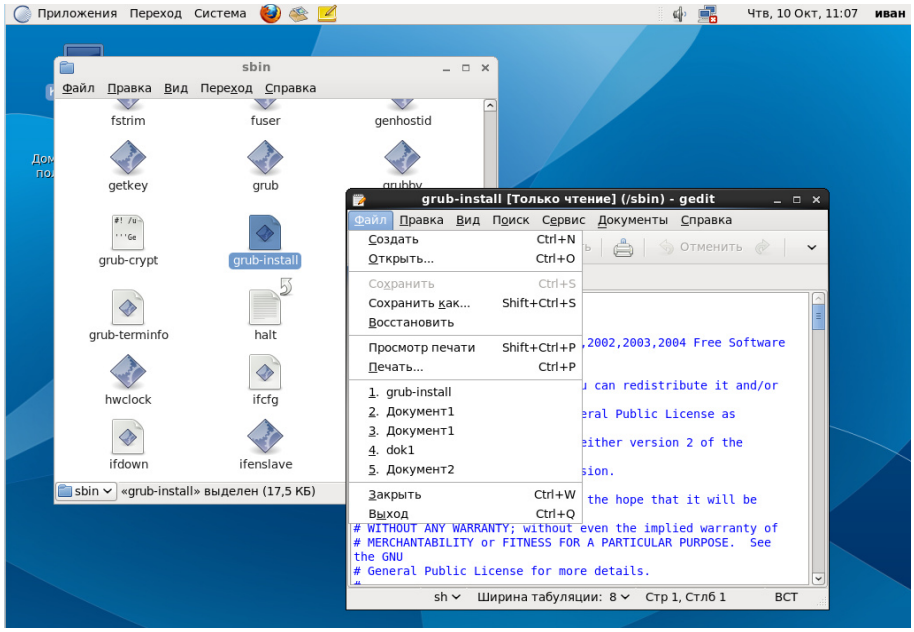


Рисунок 47 - Тип доступа для пользователей «Только чтение»

Если в блоке «Остальные» выбрать «Чтение и запись», то пользователи смогут работать с этим файлом без ограничений в правах, а если в блоке «Остальные» выбрать «Нет», то у пользователя не будет доступа к этому файлу - выведется предупреждающее сообщение.

Типы доступа для папок, которые могут быть установлены:

- «Только перечисление файлов» – указанному пользователю будет доступен перечень файлов выбранной директории;
- «Доступ к файлам» – указанному пользователю будут доступны файлы выбранной директории;
- «Создание и удаление файлов» – указанному пользователю будут доступны операции создания и удаления файлов выбранной директории;
- «Нет» – нет доступа к выбранной директории.

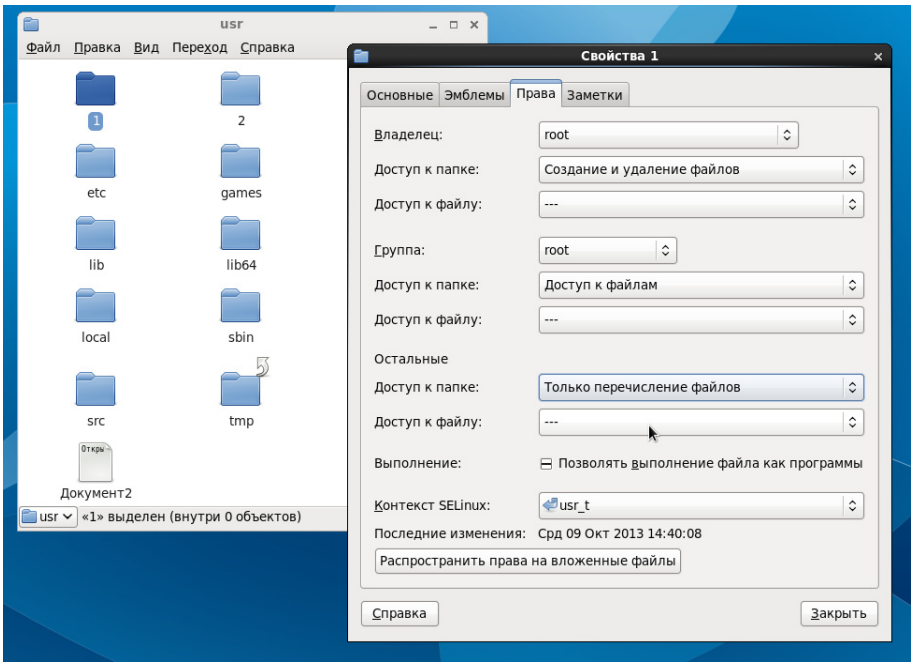


Рисунок 48 - Определение типа доступа к папке

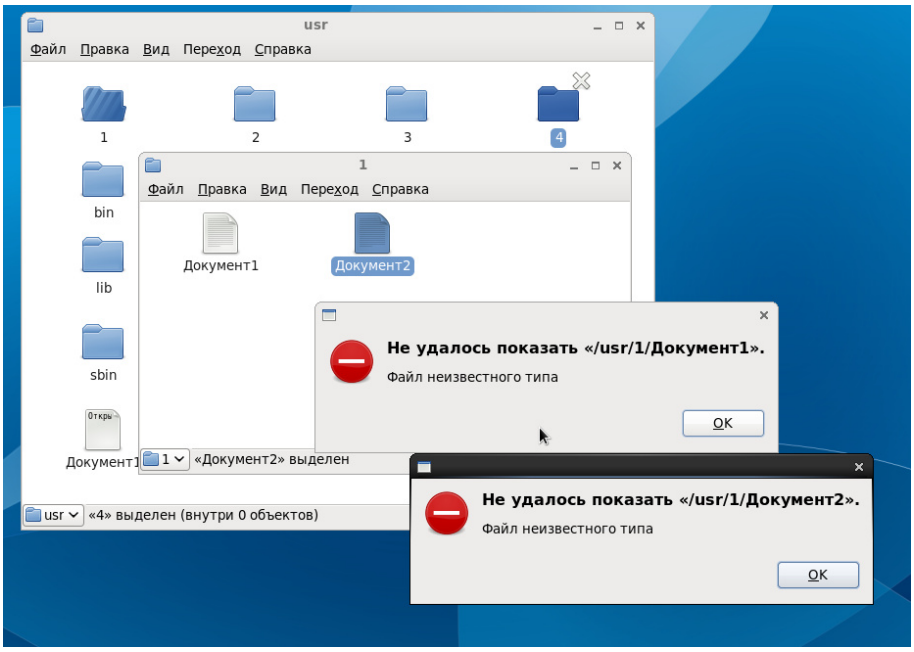


Рисунок 49 – Тип доступа "Только перечисление файлов"

4.3 Списки контроля доступа

МСВСфера 6.3 АРМ предоставляет поддержку ACL для описания контроля доступа, ориентированного на пользователя. ACL поддерживаются для всех объектов следующих файловых систем:

- ext4
- tmpfs

Запись ACL содержит следующую информацию:

- тип тега, определяющий тип записи ACL;
- квалификатор, определяющий экземпляр типа записи ACL;
- набор прав дискреционного доступа для процессов с заданным типом тега и квалификатором.

Для определения списков управления доступом ACL, установленных по умолчанию, для файла необходимо выполнить команду getfacl <имя_файла>. Пример выполнения команды на файле aide.conf приведен на рис. 50.

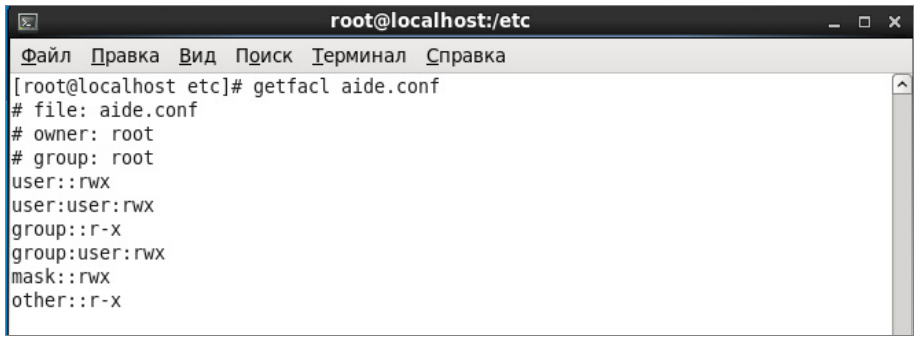


Рисунок 50 - Списки управления доступом ACL,
установленные по умолчанию для файла aide.conf

На рис. 50 видно, что компоненты списка управления доступом ACL имеют следующие значения:

ACL_USER_OBJ

user::rwx

ACL_GROUP_OBJ

group::rwx

ACL_OTHER

other::r-x

ACL_USER

user:user:rwx

ACL_GROUP

group:user:rwx

ACL_MASK

mask::rwx

Это означает, что пользователь-владелец (ACL_USER_OBJ), пользователи группы-владельца (ACL_GROUP_OBJ), пользователь user (ACL_USER) и пользователи группы user (ACL_GROUP) имеют права доступа "rwx" (чтение, запись и выполнение) к файлу aide.conf; остальные пользователи (ACL_OTHER) имеют права "r-x" (чтение и выполнение); максимальные права с которыми возможен доступ (ACL_MASK) "rwx" (чтение, запись и выполнение).

Для установки компонента ACL_USER для файла, необходимо воспользоваться командой setfacl.

setfacl -<опции> <ACL_структура>, <ACL_структура>,...,<ACL_структура> <имя_файла> <имя_файла> ...

ACL-структура представляет собой одну из следующих конструкций:

1. Конструкция определяет режим доступа к файлу или каталогу пользователя. Если пользователь не указан, определяет режим доступа пользователя-владельца.

[d[efault]:][u[ser]:][пользователь] [:[+|^]режимы_доступа]

2. То же, что и предыдущая конструкция, но для группы (ACL_GROUP_OBJ или ACL_GROUP).

[d[efault]:] g[roup]:[группа] [:[+|^]режимы_доступа]

3. Конструкция определяет действующие права доступа (ACL_MASK).

[d[efault]:] m[ask] [:[+|^] режимы_доступа]

4. Конструкция определяет режим доступа для остальных пользователей (ACL_OTHER).

[d[efault]:] o[ther] [:[+|^] режимы_доступа]

Присутствие компонента d (default) в конструкции указывает, что устанавливается Default ACL. При указании режима доступа без модификаторов (+ и ^), предыдущий режим доступа заменяется указанным в конструкции. При использовании модификатора + указанный режим доступа добавляется к существующему, при использовании ^ - удаляется. При использовании нескольких ACL-конструкции в строке запуска они разделяются запятыми. Примеры:

1. Определяет режим доступа к файлу (каталогу) для пользователя-владельца на чтение, запись и запуск (просмотр).

u::rwx

2. Добавляет к правам группы users доступ на запись.

g:users:+w

3. У пользователя user1 не будет доступа к файлам (каталогам), которые будут создаваться в указанном в командной строке каталоге.

d:u:user1:^rwx

d:u:user1:---

4. Определяет режим доступа к файлу (каталогу) остальных пользователей - чтение и запуск (просмотр).

o:r-x

o:rx

5. Убирает из действующих прав доступ на запись.

m:^w

Для установки и изменения ACL используются следующие опции:

-s Заменяет полностью ACL файла на указанный в командной строке.

-m Изменяет режимы доступа к файлу (каталогу).

-x Убирает правила доступа из ACL.

Для примера выполним установку нескольких компонентов ACL.

1. Установим компонент ACL_USER для файла aide.conf для пользователя user в значение «r-x» (рис. 51), тем самым пользователь не будет иметь право на запись файла, но сможет читать и выполнять файл (рис. 52).

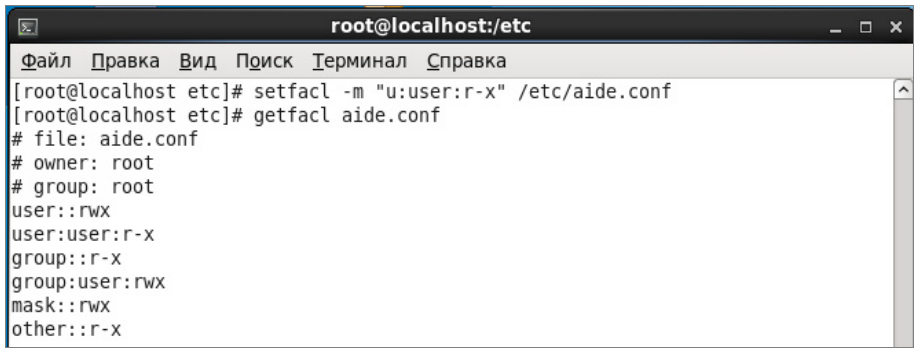


Рисунок 51 - Компонент ACL_USER для пользователя user установлен в «r-x»

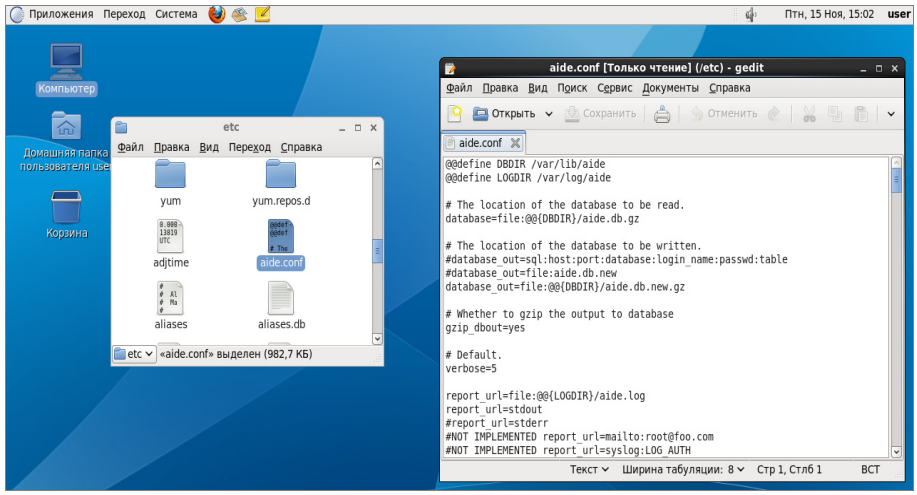


Рисунок 52 - Демонстрация результата модификации компонента ACL_USER

2. Установим компонент ACL_GROUP для файла aide.conf для группы user1 в значение «---» (рис. 53), тем самым пользователь user1, который входит в группу, не будет иметь доступ к файлу (рис. 54).

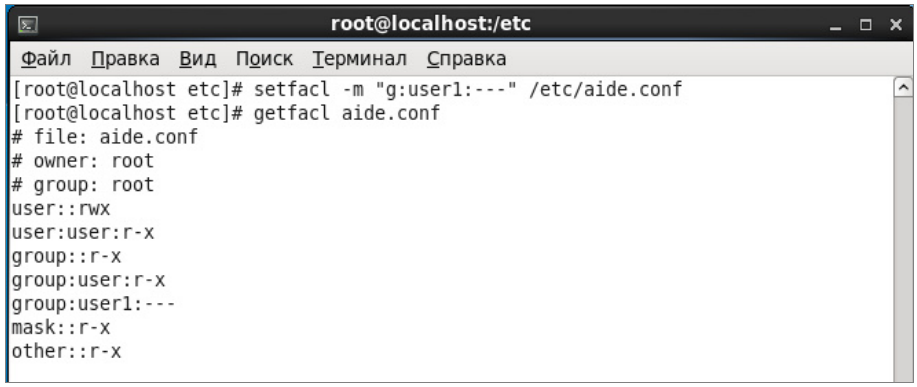


Рисунок 53 - Компонент ACL_ GROUP для группы user1 установлен в «---»

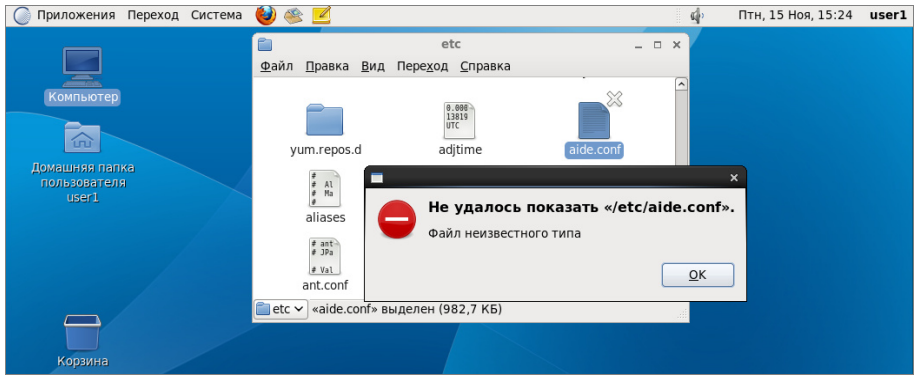


Рисунок 54 - Демонстрация результата модификации компонента ACL_ GROUP

3. Установим компонент ACL_USER для файла aide.conf для пользователя user в значение «rwx» и компонент ACL_MASK для файла aide.conf в «r--» (рис. 55), тем самым пользователь не сможет записывать и выполнять файл, хотя будет иметь на это право (рис. 56).

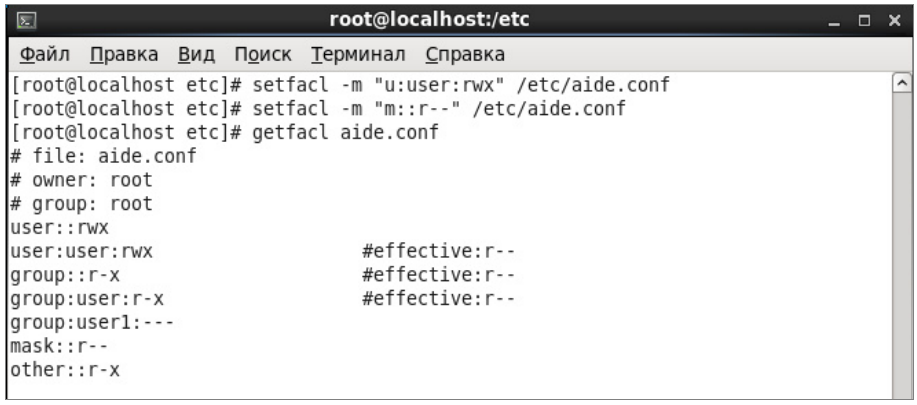


Рисунок 55 - Компонент ACL_USER установлен для пользователя user в значение «rwx» и компонент ACL_MASK установлен в «r--»

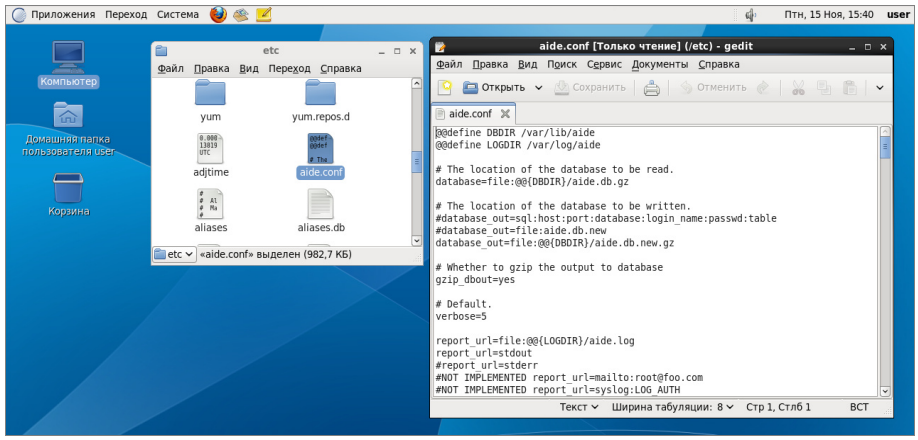


Рисунок 56 - Демонстрация результата модификации компонента ACL_MASK

4. Установим компонент ACL_USER_OBJ (пользователь-владелец user) для файла /home/user/aide/list.txt в значение «r--» (рис. 57), тем самым пользователю user файл будет доступен только для чтения (рис. 58).

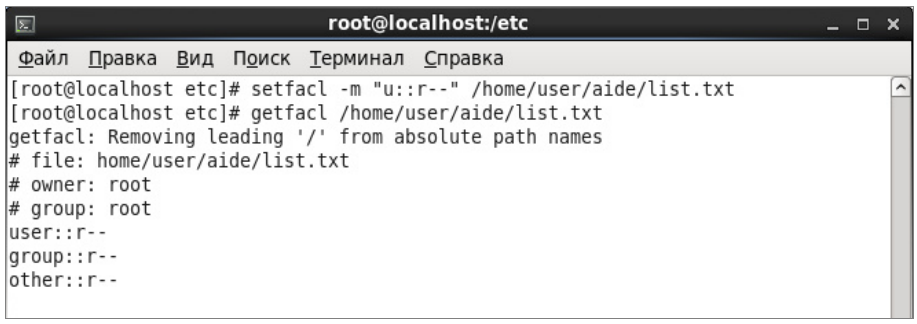


Рисунок 57 - Компонент ACL_USER_OBJ установлен для пользователя-владельца user в значение «r--»

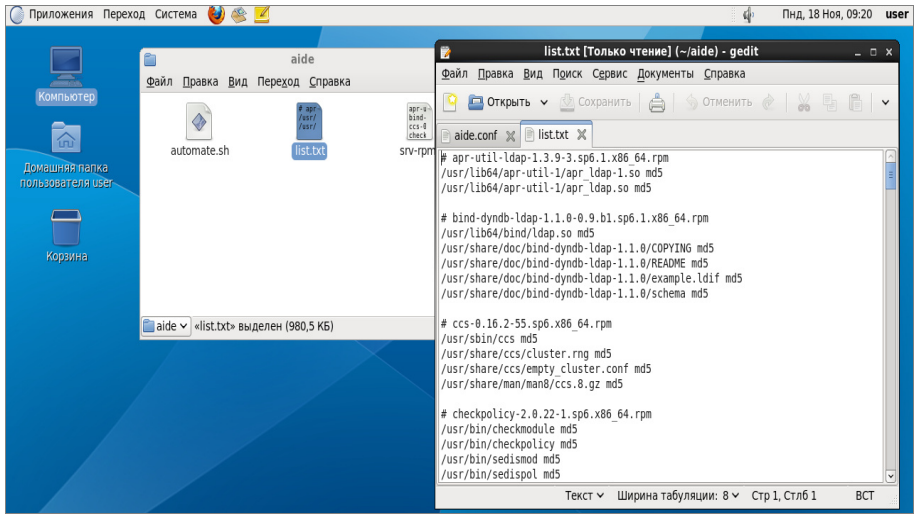


Рисунок 58 - Демонстрация результата модификации компонента ACL_USER_OBJ

5. Установим компонент ACL_OTHER для файла /etc/aide.conf в значение «---» (рисунок 59), тем самым всем пользователям, кроме владельца root, файл будет не доступен, например, пользователям user и user1 (рис. 60 и рис. 61).

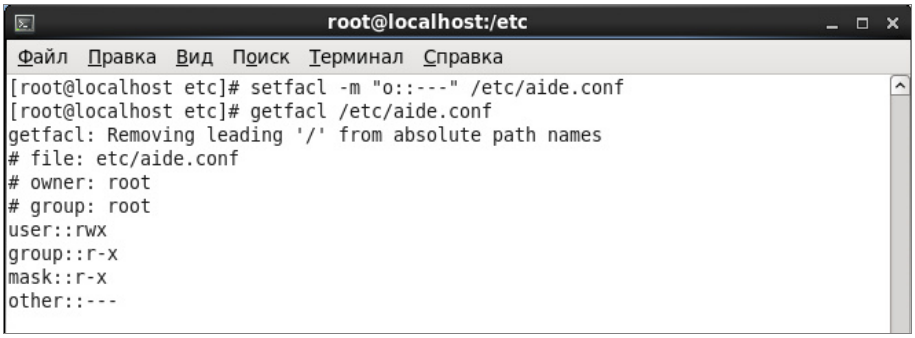


Рисунок 59 - Компонент ACL_OTHER установлен для всех пользователей, кроме владельца (root), в значение «---»

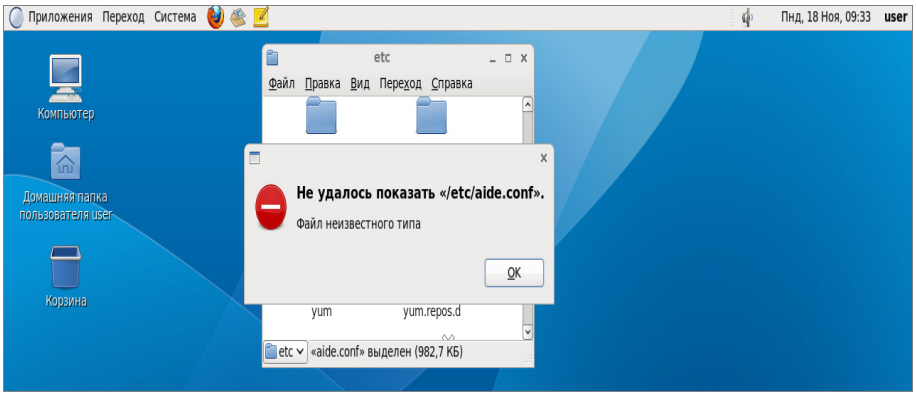


Рисунок 60 - Демонстрация результата модификации компонента ACL_OTHER для пользователя user

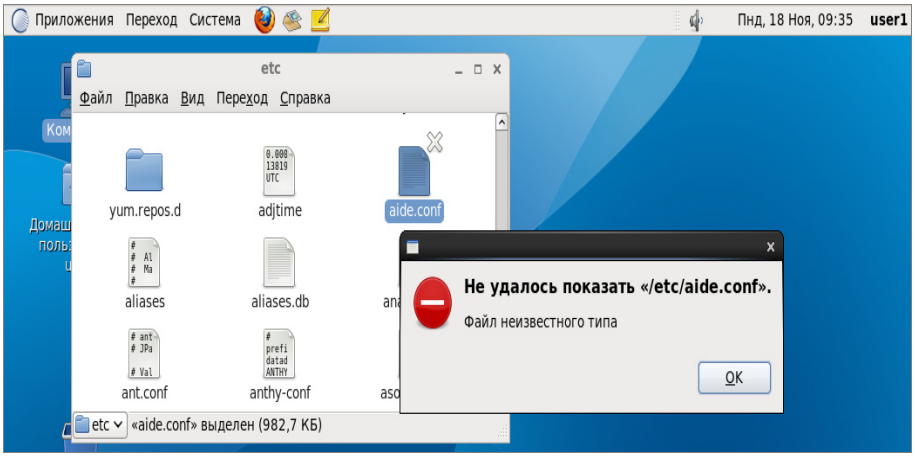


Рисунок 61 - Демонстрация результата модификации компонента ACL_OTHER для пользователя user1

4.4 Приложение "Менеджер пользователей"

Управление учетными записями пользователей может осуществляться в приложении «Менеджер пользователей», которое запускается из меню «Система–>Администрирование–>Пользователи и группы».

Для создания учетной записи пользователя необходимо нажать кнопку "Добавить пользователя" в приложении «Менеджер пользователей». В появившемся окне (рис. 62) нужно обязательно указать имя учетной записи, полное имя пользователя, пароль, оболочку, домашний каталог и при необходимости можно создать частную группу пользователя, которая будет иметь одноименное название с учетной записью, указать ID пользователя и группы вручную (по умолчанию ID пользователя и группы задаются в порядке возрастания). После заполнения всех полей, нужно нажать кнопку "ОК" и новая учетная запись пользователя появится в списке.

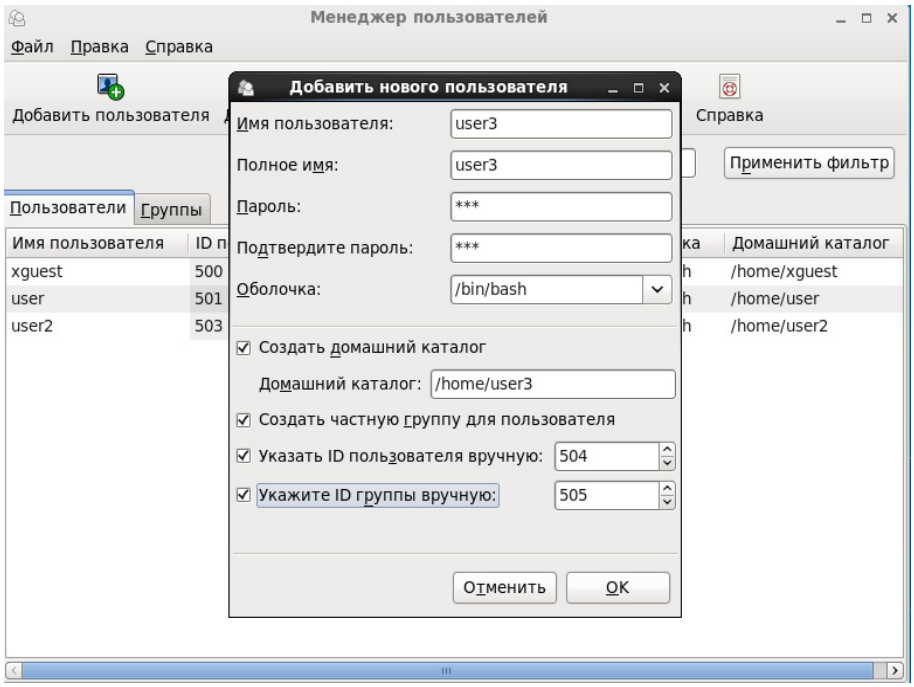


Рисунок 62 - Добавление нового пользователя

Для изменения пароля пользователем при входе в систему нужно настроить в свойствах учетной записи на вкладке "Сведения о пароле" пункты "Ограничить срок действия пароля" и "Изменить пароль при следующей авторизации" (рис. 63).

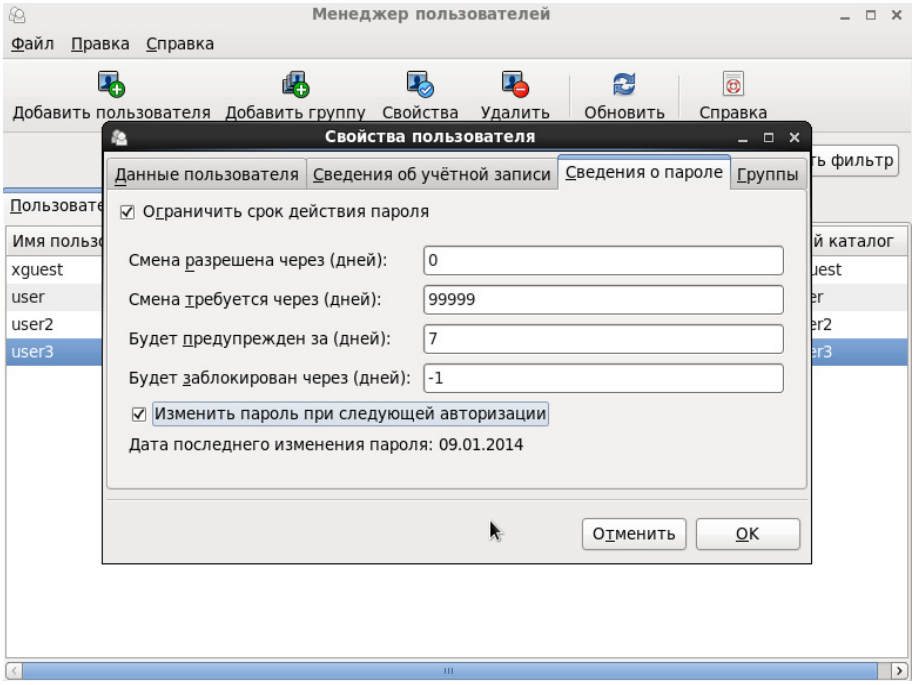


Рисунок 63 - Настройка изменения пароля при авторизации

Тем самым при авторизации пользователь должен будет сменить пароль. Это удобно использовать при активации учетной записи. Т.к. учетная запись создается на уровне привилегий root, то пользователь для входа получает уже готовый пароль, а настроив изменение пароля при авторизации, пользователь может задать свой пароль для учетной записи.

Для этого при входе в систему пользователь сначала вводит пароль, заданный администратором (рис. 64), затем указывает текущий пароль (рис. 65) и после этого вводит новый пароль (рис. 66).

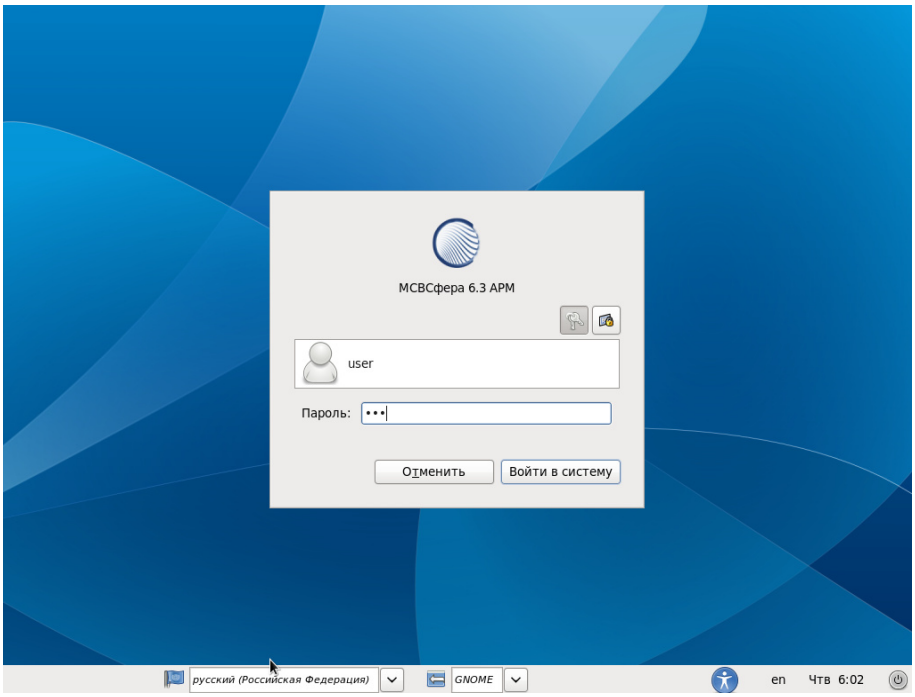


Рисунок 64 - Ввод пароля при входе в систему

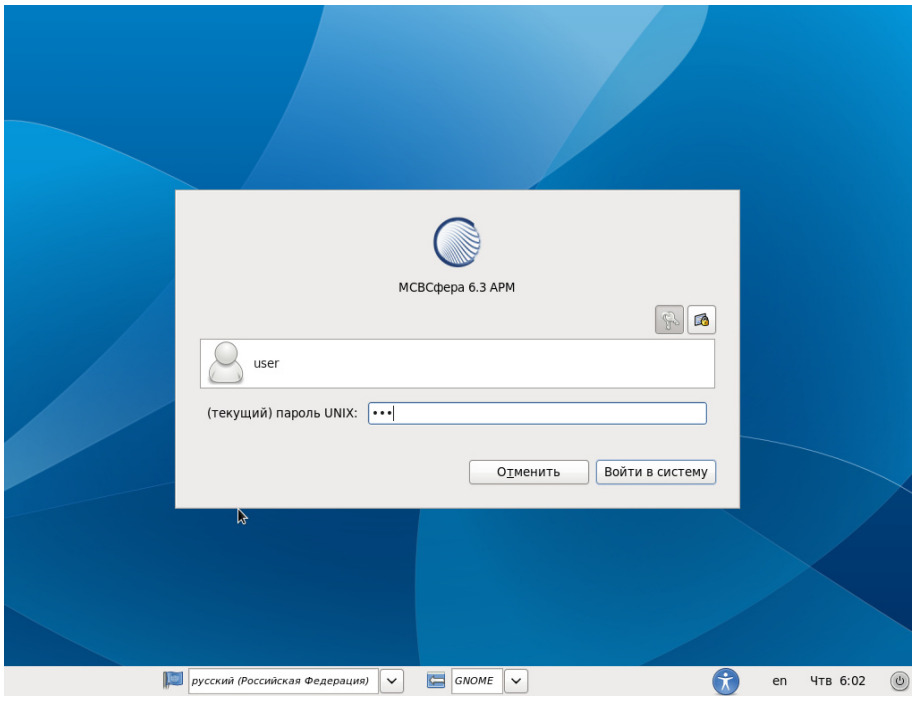


Рисунок 65 - Ввод текущего пароля

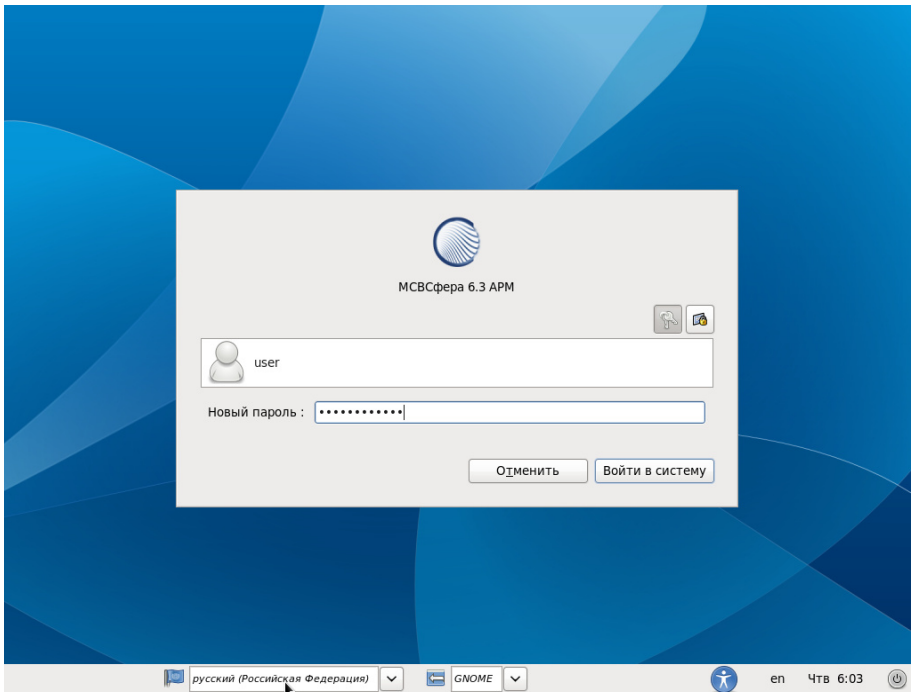


Рисунок 66 - Ввод нового пароля

Для уничтожения учетной записи нужно выбрать пользователя и нажать унопку "Удалить". В появившемся окне (рис. 67) утвердить удаление домашнего каталога пользователя, буфера почты и временных файлов, если это необходимо.

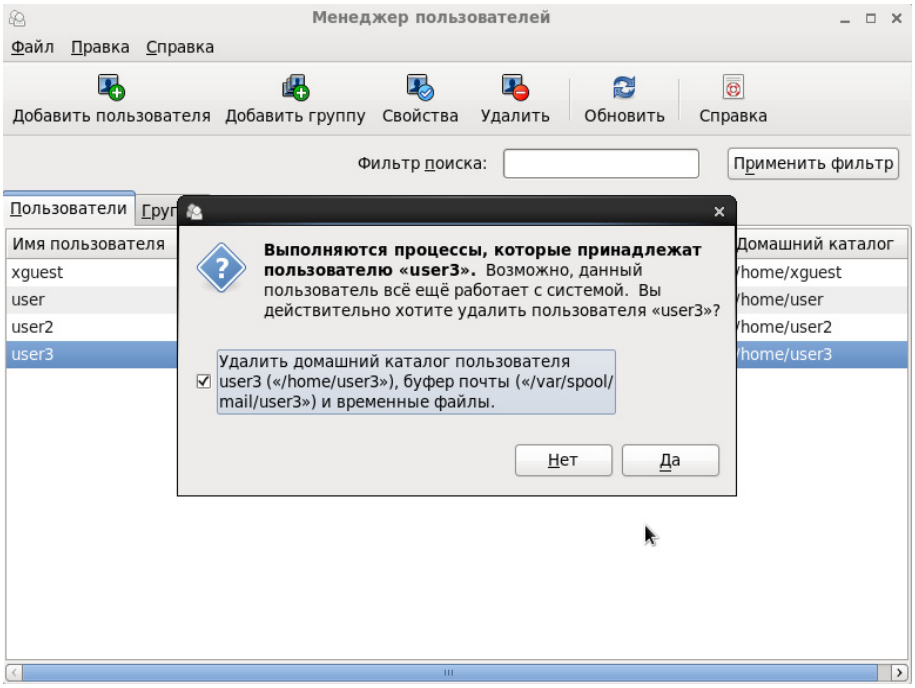


Рисунок 67 - Удаление учетной записи

Изм.	Лист	№ докум	Подп	Дата

4.5 Утилиты командной строки

Модель полномочного контроля доступа МСВСфера 6.3 АРМ реализуется с помощью SELinux. SELinux, использующий TE, служит основой для MAC. Модель MAC SELinux полностью отделяет механизм её реализации от политики безопасности. Механизм реализации расширяет традиционный механизм TE для поддержки политики безопасности.

Для того чтобы убедиться, что SELinux действительно работает, нужно использовать утилиту sestatus, как показано на рис. 68.

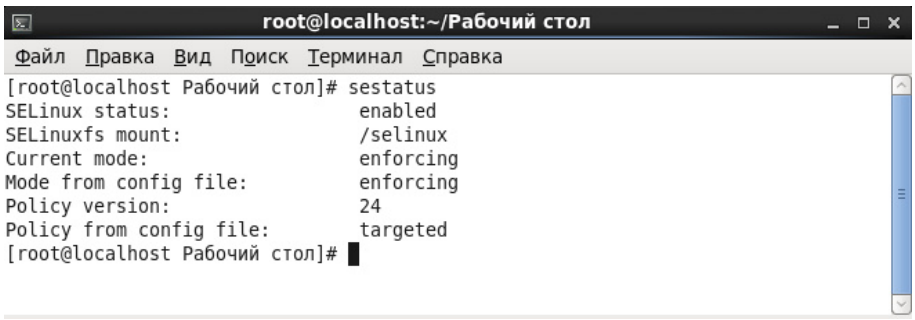


Рисунок 68 - Проверка состояния SELinux

Утилита sestatus показывает, что подсистема SELinux включена (SELinux status: enabled), задействован режим ограничений (Current mode: enforcing) и используется политика безопасности под названием targeted.

Все эти параметры устанавливаются в конфигурационном файле /etc/selinux/config. Текущий режим ограничений указывается в параметре SELINUX. Чтобы отключить SELinux, достаточно указать для этого параметра значение disabled.

Существуют три режима работы SELinux, которые могут быть указаны в соответствующем параметре конфигурационного файла:

Enforcing - выбор этого значения приводит к применению текущей политики SELinux, при этом будут блокироваться все действия, нарушающие политику, информация о заблокированных действиях заносится в журнальный файл, режим Enforcing можно изменить без перезагрузки системы.

Permissive - при указании этого параметра модулем syslog фиксируются попытки выполнения действий, противоречащих текущей политике безопасности, однако фактического блокирования действий не происходит, режим Permissive, как правило, используется для отладки правил доступа, смена этого режима на другой не требует перезагрузки.

Disabled - данное значение в параметре SELINUX файла настроек полностью отключает подсистему обеспечения мандатного контроля доступа, при включении SELinux в любом режиме необходимо заново установить метки безопасности в файловой системе (для этого необходима перезагрузка системы).

Для переключения между режимами работы Enforcing и Permissive без перезагрузки операционной системы можно использовать утилиту setenforce. Если выполнить команду setenforce enforcing или setenforce 1, то SELinux перейдет в режим Enforcing. Команда setenforce permissive или setenforce 0 переводит в режим Permissive. Такое переключение режимов не влияет на конфигурационный файл SELinux, поэтому после перезагрузки система обеспечения полномочного контроля доступа вернется к режиму, указанному в файле /etc/selinux/config (рис. 69). Также существует команда getenforce, которая выведет краткую информацию, в каком режиме работает SELinux на текущий момент (рис. 70).

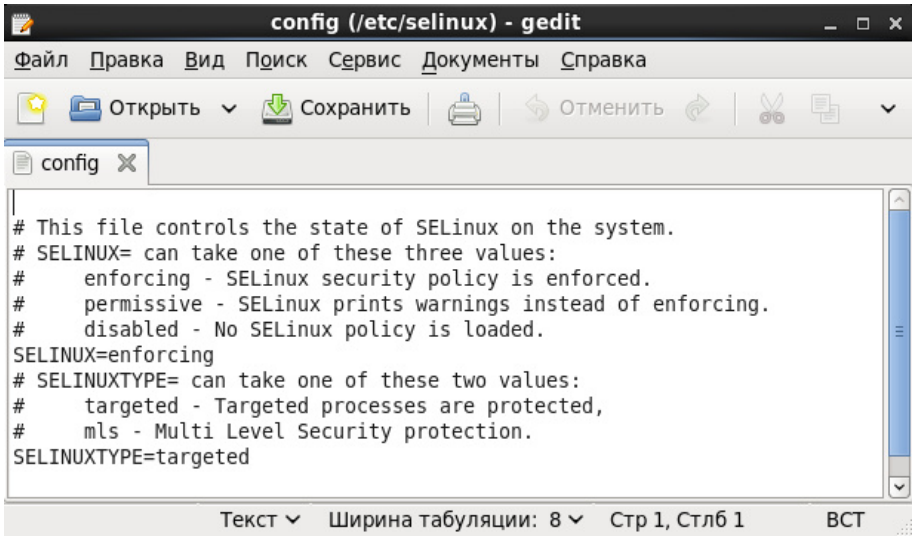


Рисунок 69 - Конфигурационный файл SELinux /etc/selinux/config

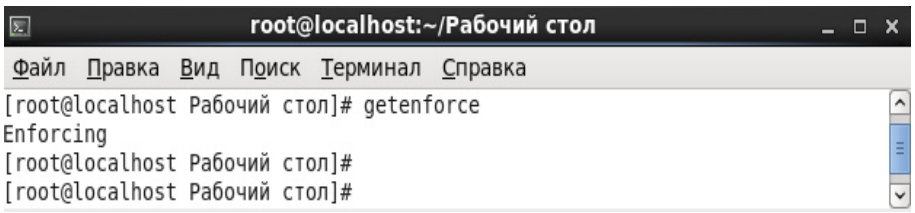


Рисунок 70 - Использование утилиты getenforce

Управление режимами работы SELinux можно осуществлять и через параметры ядра Linux. Параметр selinux=0 эквивалентен значению Disabled в конфигурации SELinux, а enforcing=0 и enforcing=1 позволяют загрузить операционную систему с SELinux, находящимся в режиме Permissive или Enforcing соответственно.

Команда semanage позволяет добавлять, изменять и удалять сопоставления между пользователями системы и SELinux-пользователями. Чтобы посмотреть, какому SELinux-пользователю по умолчанию сопоставлены пользователи системы, наберите в консоли semanage login -l | grep default (рис. 71).

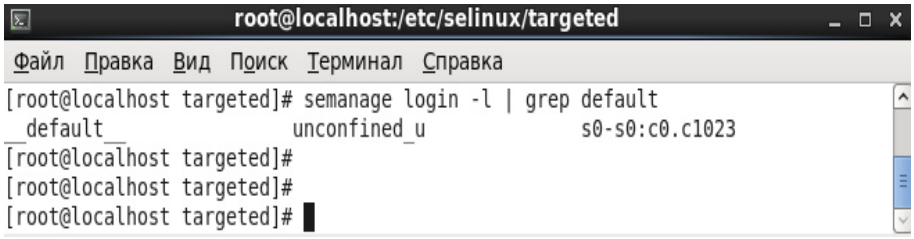


Рисунок 71 - Определение SELinux-пользователя по умолчанию

На рис. 71 видно, что пользователи системы по умолчанию сопоставлены SELinux-пользователю unconfined_u.

Чтобы переопределить данное сопоставление, нужно при добавлении пользователей в систему выполнять команду useradd**,** используя опцию -Z. Эта опция определяет, какому SELinux-пользователю должен быть сопоставлен добавляемый пользователь (рис. 72).

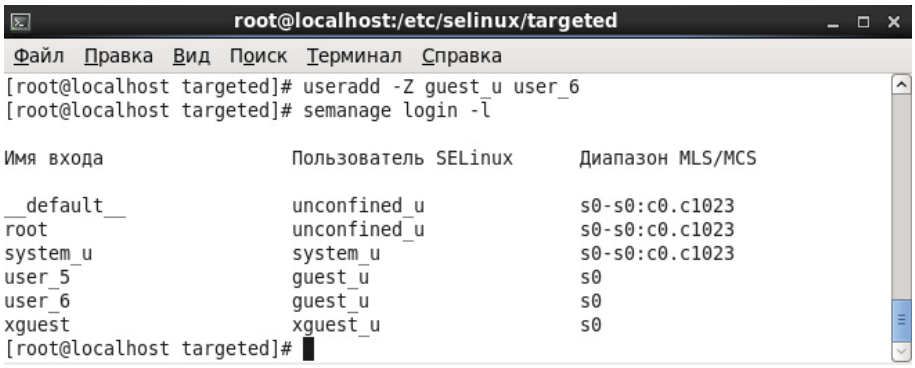


Рисунок 72 - Добавление пользователя с переопределением сопоставления

На рис. 72 видно, что создан новый пользователь с именем user_6, который будет сопоставлен SELinux-пользователю guest_u вместо определенного по умолчанию SELinux-пользователя.

Также для изменения сопоставления между пользователем системы и SELinux-пользователем может быть использована команда usermod с опцией -Z (рис. 73).

Рисунок 73 - Сопоставление между пользователем системы и SELinux-пользователем

Существует несколько предопределенных профилей SELinux-пользователей. Список данных профилей можно вывести командой semanage user -l (рис. 74).

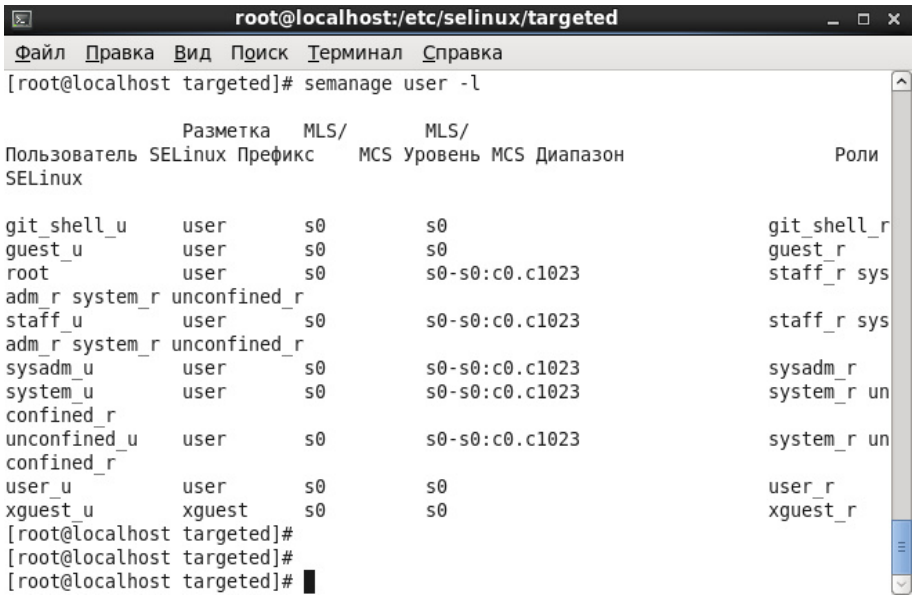


Рисунок 74 - Предопределенные профили SELinux-пользователей

Вывести список всех сопоставлений между пользователями системы и SELinux-пользователями можно командой semanage login -l (рис. 75).

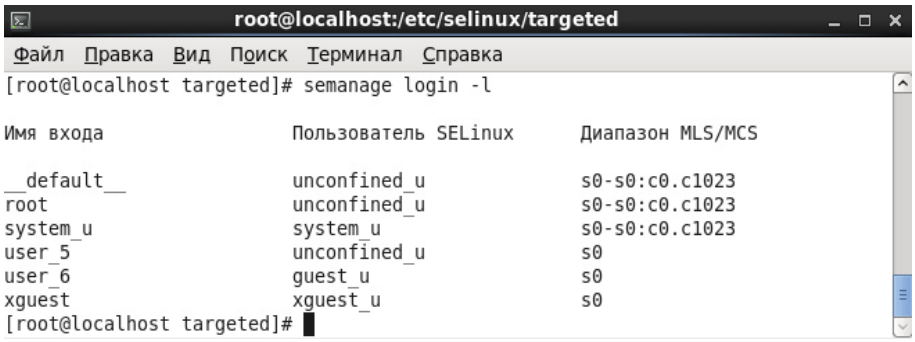


Рисунок 75 - Вывод списка всех сопоставлений

Удалить сопоставление между пользователем системы и SELinux-пользователем можно командой semanage login -d <имя_пользователя> (рис. 76).

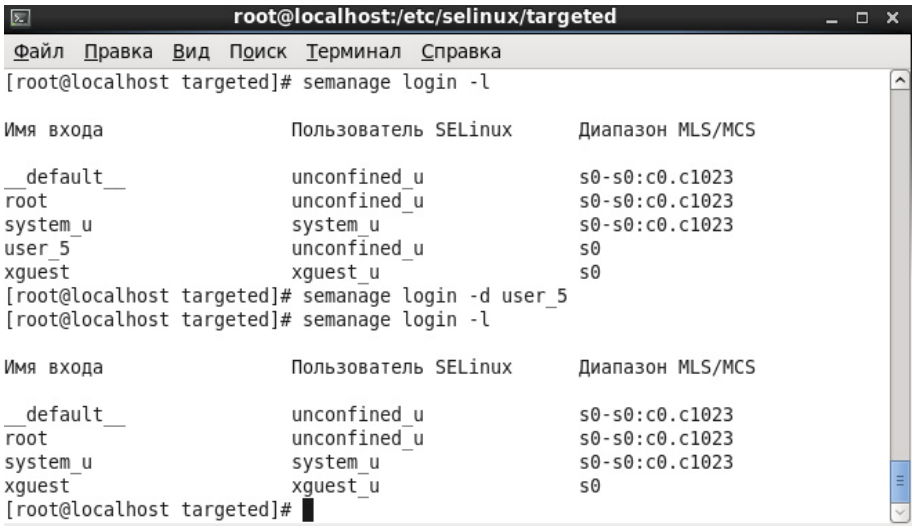


Рисунок 76 - Удаление сопоставлений

4.6 Приложение "Администрирование SELinux"

Помимо утилит командной строки настройка параметров Selinux осуществляется с помощью приложения «Администрирование SELinux», которое запускается из пункта меню "Система->Администрирование->Управление SELinux".

На вкладке "Статус" необходимо установить режим администрирования и тип политики (параметр "SELINUXTYPE" в конфигурационном файле /etc/selinux/config), как показано на рис. 77. Выбор параметров на данной вкладке зависит от целей безопасности, которые ставит перед собой администратор. Ниже по тексту представлены краткие характеристики устанавливаемых параметров.

Режим администрирования SELinux.

Поле "Строгий режим по умолчанию" может быть установлено в три значения: "Выключено" (disabled), "Разрешающий" (permissive) и "Строгий" (enforcing). Если строгий режим включен (не принимает значение "Выключено"), то поле "Текущий строгий режим" принимает значения "Строгий" (enforcing) или "Разрешающий" (permissive).

Описание режимов администрирования представлено в пункте 4.5.

Политики безопасности SELinux.

Политики безопасности для системы полномочного контроля доступа: "trageted", "mls", "strict" и "minimum" (по умолчанию "targeted").

Политика безопасности targeted. Ее цель - защитить операционную систему от системных процессов, передающих и получающих сообщения через сетевые сервисы (например, NFS, DNS, HTTP). Эти процессы являются наиболее частыми объектами для атак злоумышленников, так как присутствуют практически на любом сервере и, как правило, выполняются с полномочиями пользователя root.

Политика безопасности MLS**.** Этот режим доступен, если установлены следующие пакеты: mcstrans, policycoreutils-newrole, selinux-policy-mls. Многоуровневая безопасность (Multilevel security или Multiple Levels of Security — MLS) — это система разделения уровней доступа по различным уровням важности информации (т.е. различным уровням безопасности), что позволяет оградить важную информацию от работников с низким уровнем доступа. Политика MLS содержит не только правила, указывающие, какие объекты системы безопасности могут совершать определенные действия, и что они могут сделать, находясь на определенном уровне безопасности. В MLS также существуют две дополнительные характеристики уровня безопасности: важность (sensitivity), выражающаяся в диапазоне от s0 до s15, и возможности (capabilities) — от c0 до c255. Это дает дополнительные возможности для реализации многоуровневой системы безопасности на основе SELinux.

Политика безопасности strict. Этот режим доступен, если установлен пакет selinux-policy-strict. Политика strict - наиболее строгая из всех стандартных политик безопасности. Она ограничивает деятельность не только системных, но и пользовательских процессов. Если установить политику strict и режим Enforcing, то станет невозможно (даже с полномочиями root) просмотреть журнальные файлы, сменить режим работы на Permissive или совсем отключить SELinux. Пользователь даже не сможет корректно перезагрузить компьютер. Единственным выходом станет нажатие кнопки Reset на компьютере (или сигнал завершения от системы виртуализации) и установка параметра ядра enforcing=0 или selinux=0.

Политика безопасности minimum. Этот режим доступен, если установлен пакет selinux-policy-minimum. Политика безопасности minimum была разработана на основе политики targeted специально для пользователей, желающих потренироваться в создании собственных политик для SELinux. Политика minimum содержит те же модули, что и политика targeted, однако не задействует их. Изначально SELinux не ограничивает никакие объекты системы безопасности, но при желании можно, например, установить модули для контроля процессов. В этом случае потребуется явно настроить необходимые разрешения в политике безопасности. Тем не менее, политика minimum является хорошей «песочницей» для проведения экспериментов с SELinux.

В каталоге /etc/selinux для каждой из политик создаются подкаталоги, в которых располагаются соответствующие конфигурационные файлы.

После смены установленного параметра ("Тип политики по умолчанию") потребуется перезагрузка системы. Для того чтобы при загрузке SELinux автоматически расставил в файловой системе необходимые метки, соответствующие политике безопасности, необходимо установить галочку для поля "Переразметка при следующей загрузке".

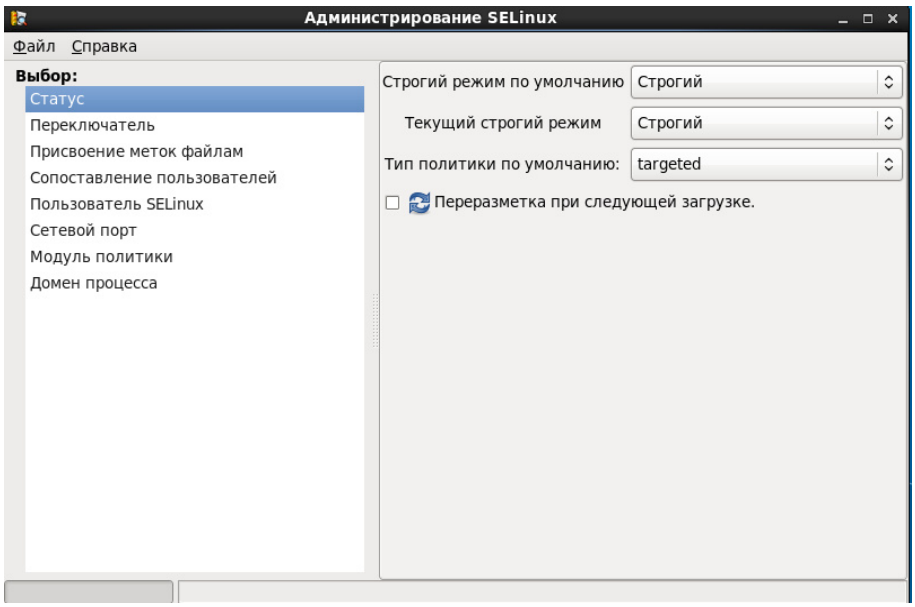


Рисунок 77 - Окно приложения "Администрирование SELinux", вкладка "Статус"

Изм.	Лист	№ докум	Подп	Дата

На вкладке "Переключатель" выполняется настройка ленты конфигурации SELinux (рис. 78). Переключатели - это блоки политики, которые можно добавлять или удалять на лету, переключая их значение. Почти каждое правило, добавляемое в политику SELinux, добавляет новые привилегии. Для максимального повышения безопасности, обеспечиваемой SELinux, число активных правил следует минимизировать. Иногда политика добавляется включением переключателя, а иногда - выключением. Описание переключателя можно просмотреть в исходном тексте политики.

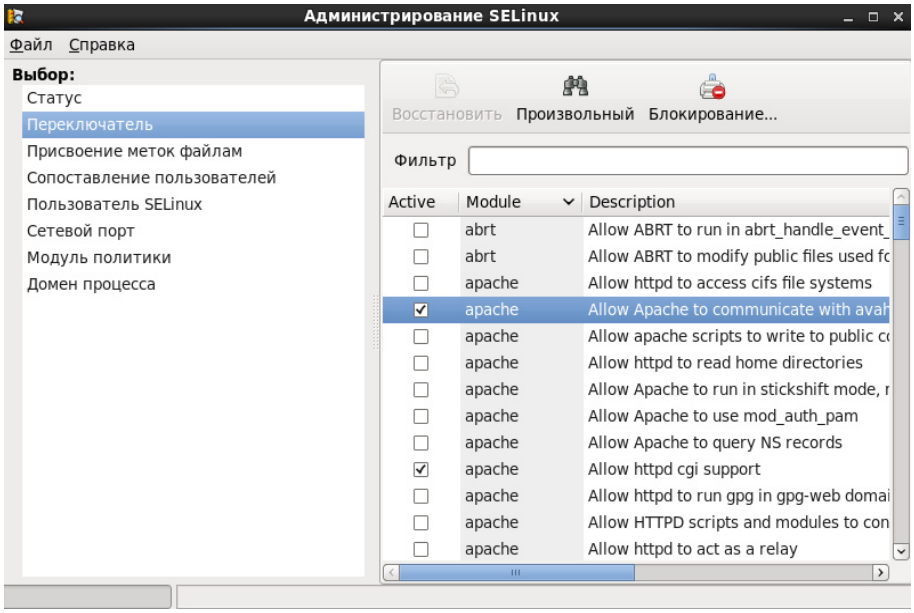


Рисунок 78 - Окно приложения "Администрирование SELinux"
вкладка "Переключатель"

SELinux позволяет блокировать логические переменные, относящиеся к блокам политик на вкладке "Переключатель". Для вызова окна "SELinux Boolean Lockdown" ("Мастер блокировки логических переменных") нужно выбрать переключатель и нажать кнопку "Блокирование...". В открывшемся окне (рис. 79) можно разблокировать (Enabled), заблокировать (Disabled) и восстановить значение по умолчанию для переменной (Default).

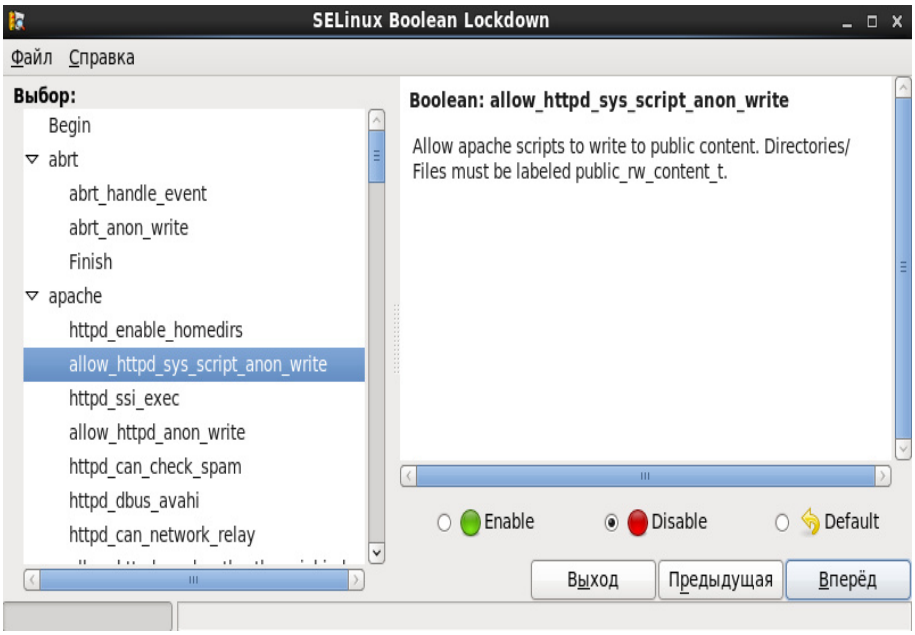


Рисунок 79 - Мастер блокировки логических переменных

Вкладка "Присвоение меток файлам" позволяет настраивать SELinux типы файлов (метки) файлам и группам файлов (рис. 80). Метки чувствительности состоят из иерархической части (уровень) и неиерархического набора категорий. Модуль безопасности SELinux приписывает "метку чувствительности" объектам как часть контекста защиты. Метки файлов можно добавлять (кнопка "Добавить"), удалять (кнопка "Удалить"), изменять (кнопка "Свойства" для выбранной метки), а так же фильтровать (выбрав Произвольный фильтр). Примечание: эти метки чувствительности не присваиваются виртуальным машинам и их ресурсам.

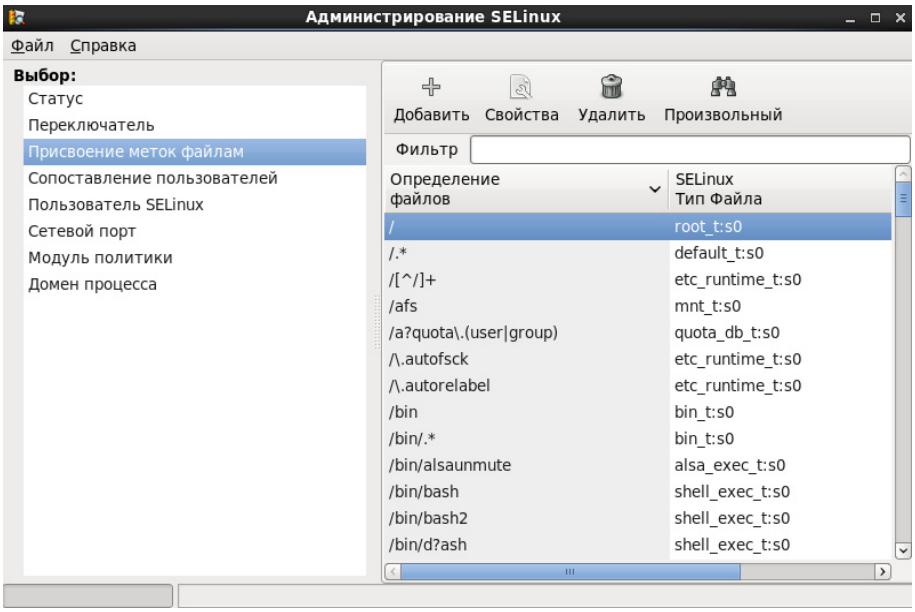


Рисунок 80 - Окно приложения "Администрирование SELinux"
вкладка "Присвоение меток файлам"

На рис. 81 приведено окно настройки сопоставления пользователей. Пользователи системы по умолчанию сопоставляются SELinux-пользователю unconfined_u. Сопоставление пользователей можно добавлять (кнопка "Добавить"), удалять (кнопка "Удалить"), изменять (кнопка "Свойства" для выбранной метки), а так же фильтровать, задав фильтр в соответствующем поле.. Далее приведем описание свойств, предопределенных SELinux-пользователей.

Свойства предопределенных SELinux-пользователей.

SELinux-пользователь guest_u:

Этот профиль используется для пользователей, которых необходимо усиленно контролировать. SELinux-пользователь guest_u может только войти в систему, используя OpenSSH. Гостевые пользователи не имеют доступа к сетевым ресурсам и программам с установленными битами setuid и setgid.

SELinux-пользователь xguest_u:

Данный профиль аналогичен guest_u за исключением того, что xguest пользователи могут входить в Xwindow и не могут входить, используя OpenSSH. Другим исключением является то, что данный пользователь может получить доступ к HTTP порту, используя контролируемый SELinux экземпляр Mozilla Firefox.

SELinux-пользователь user_u:

SELinux-пользователь user_u напоминает обычного непривилегированного ограниченного (confined) SELinux-пользователя. Такой пользователь может войти в систему, используя Xwindow и OpenSSH, имеет доступ к сетевым ресурсам, но не может использовать программы с установленными битами setuid и setgid.

SELinux-пользователь staff_u:

Этот SELinux-пользователь идентичен user_u, за исключением того, что staff_u может использовать программы с флагами setuid и setgid. Кроме того, пользователь staff_u может также просмотреть информацию обо всех процессах в системе и имеет некоторые другие несущественные привилегии по сравнению с пользователем user_u.

SELinux-пользователь sysadm_u:

Данный пользователь придуман, чтобы ограничить, используя SELinux, учетную запись root, что обычно делать не рекомендуется. Он используется в Multi Level Security окружении, где нет пользователя unconfined_u.

SELinux-пользователь unconfined_u:

SELinux-пользователь unconfined_u - это среда, в которой по умолчанию работают все Linux-пользователи в соответствии с целевой политикой. Этот пользователь в значительной степени освобожден от ограничений, накладываемых SELinux. Исключением является механизм Memory Execution Protections (ограничение на исполнение определенных операций в памяти).

SELinux-пользователь system_u:

Этот пользователь зарезервирован для нужд системы. Обычные Linux-пользователи не должы сопоставляться с SELinux-пользователем system_u.

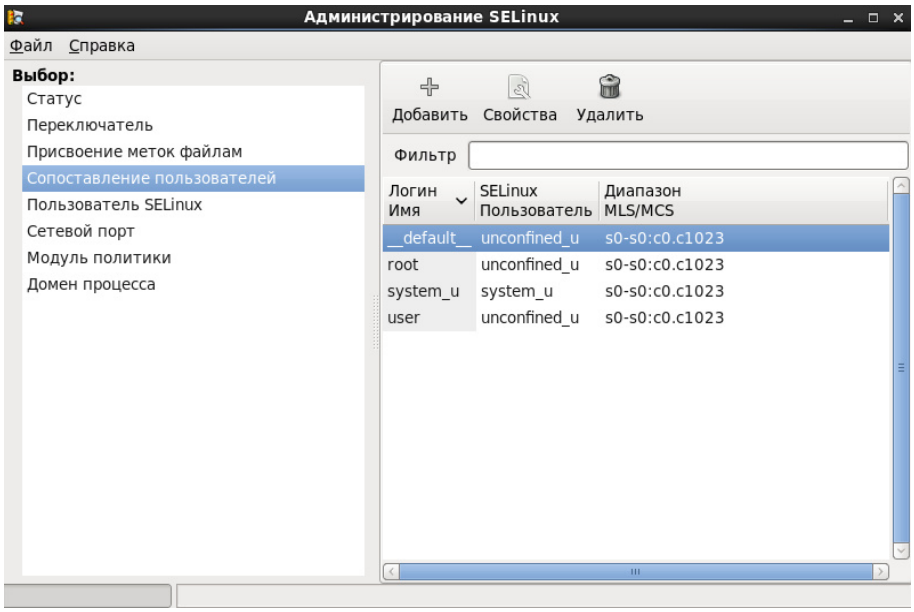


Рисунок 81 - Окно приложения "Администрирование SELinux" вкладка "Сопоставление пользователей"

Окно настройки свойств SELinux пользователей приведено на рис. 82. Пользователей SELinux можно добавлять (кнопка "Добавить"), удалять (кнопка "Удалить"), изменять (кнопка "Свойства" для выбранной метки), а так же фильтровать, задав фильтр в соответствующем поле.

SELinux-пользователь, сопоставляемый пользователям по умолчанию, unconfined_u сопоставлен ролям unconfined_r и system_r и всем доступным категориям (compartments). Обе роли unconfined_r и system_r сопоставляются доменам безопасности SELinux. Домены безопасности SELinux - это определенные окружения безопасности для процессов в системе Linux. Неограниченный домен безопасности - unconfined_t - зарезервированное окружение для процессов, которые в значительной степени освобождены от ограничений SELinux. Роль system_r сопоставляется доменам безопасности для системных процессов. SELinux-пользователь unconfined_u имеет доступ к роли system_r, чтобы иметь возможность запускать системные процессы в своих доменах безопасности. SELinux-пользователь unconfined_u работает в домене безопасности unconfined_t через роль unconfined_r, которой он сопоставлен.

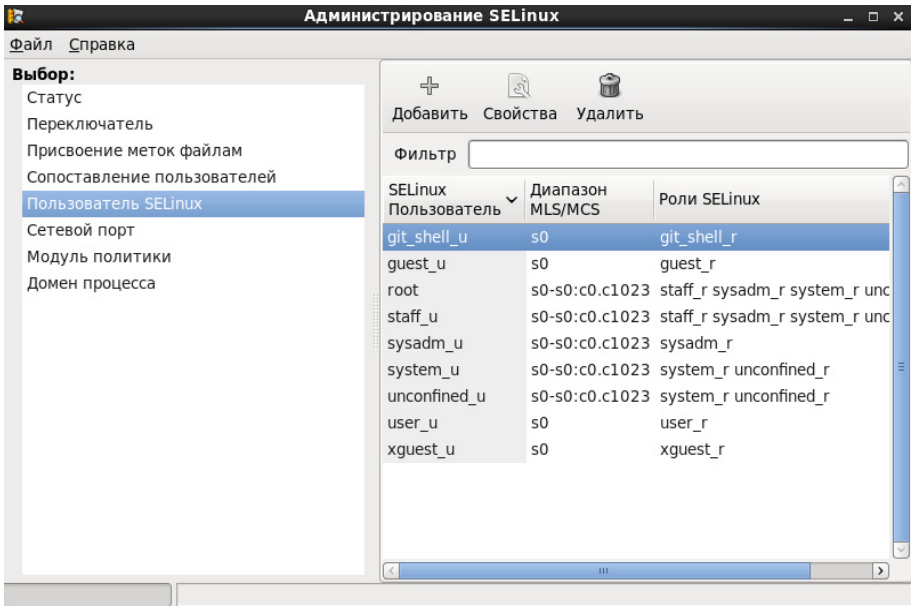


Рисунок 82 - Окно приложения "Администрирование SELinux"
вкладка "Пользователь SELinux"

На следующем рисунке приведена вкладка "Сетевой порт". В окне можно настроить тип SELinux порта, протокол и MLS/MCS уровень для сетевого порта. SELinux параметры портов можно задавать относительно списков (рис. 83) и груп (рис. 84).

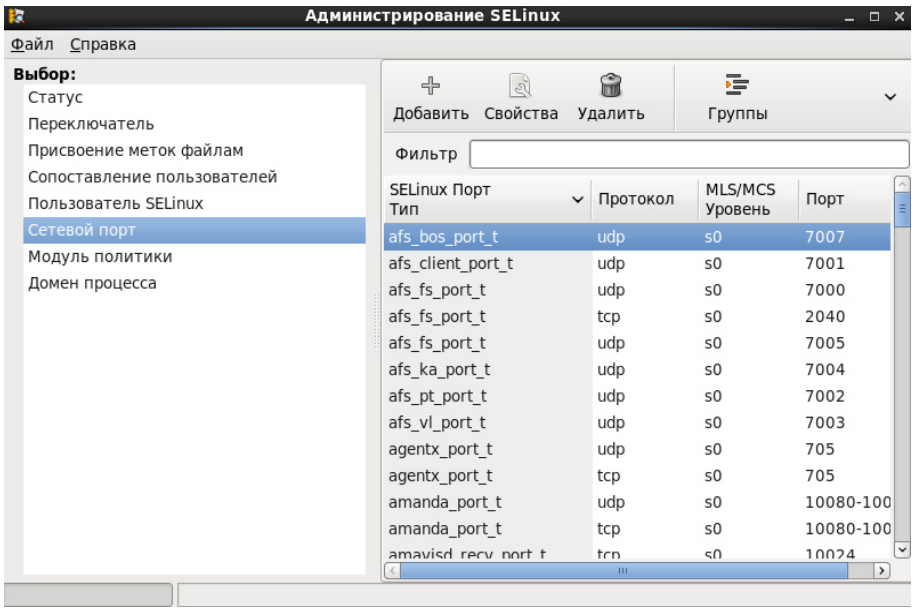


Рисунок 83 - Окно приложения "Администрирование SELinux",
вкладка "Сетевой порт" для списка

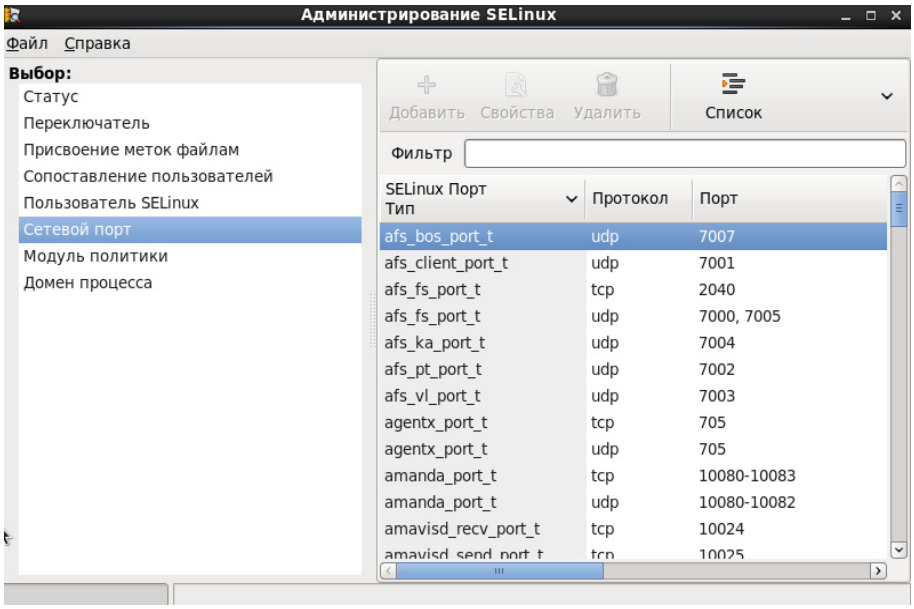


Рисунок 84 - Окно приложения "Администрирование SELinux", вкладка "Сетевой порт" для групп

На вкладке "Модуль политики" можно создать (кнопка "Создать"), добавить (кнопка "Добавить"), удалить (кнопка "Удалить") модули политики и включить SELinux аудит (кнопка "Включить аудит") (рис. 85).

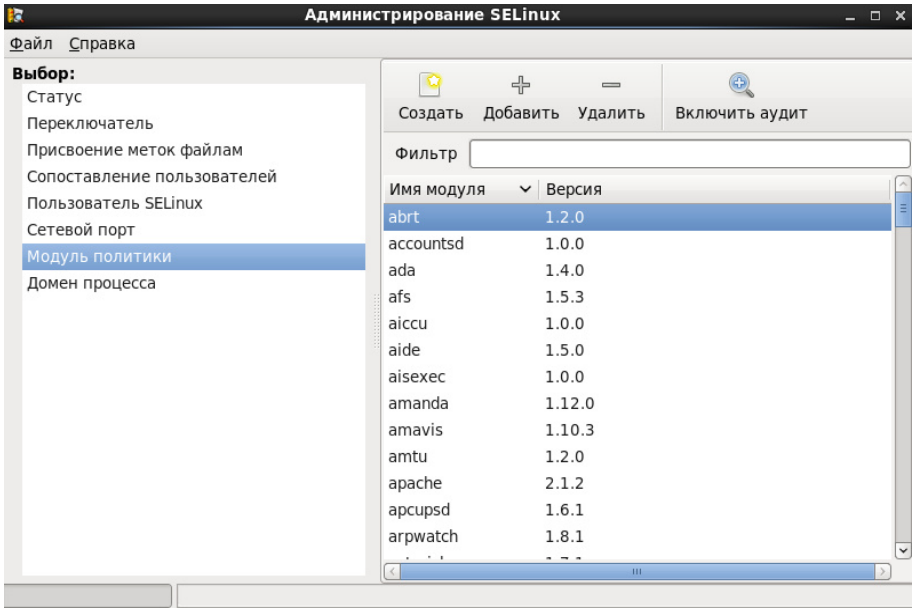


Рисунок 85 - Окно приложения "Администрирование SELinux" вкладка "Модуль политики"

На рис. 86 представлено окно настройки доменов процесса, для которых можно задать или отменить разрешающий режим.

Разрешающие домены могут быть использованы для:

1) перевода работы определенного процесса (домена) в разрешающий режим для анализа и выявления проблем, вместо подвержения риску целой системы, за счет перевода системы в разрешающий режим;

2) создания политик для нового приложения - в новой политике помечаются только определенные домены как разрешающие, без риска уязвимости всей системы.

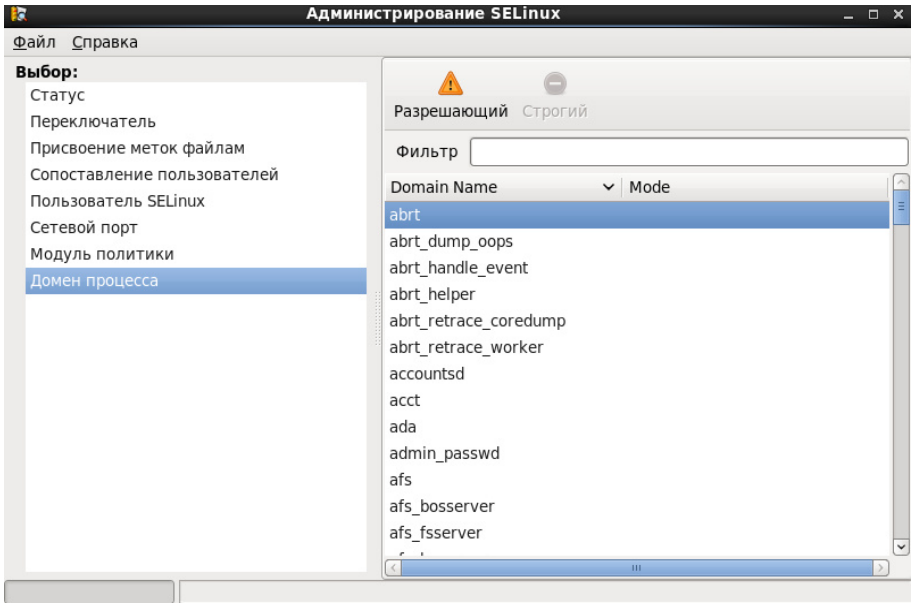


Рисунок 86 - Окно приложения "Администрирование SELinux"
вкладка "Домен процесса"

4.7 Конфигурационный файл /etc/sudoers

Используя команду sudo, авторизованные администраторы могут утвердить действия других пользователей. Как только администратор утверждает операцию, изменяется файл /etc/sudoers, чтобы предоставить пользователю право выполнения административной операции.

Используя команду sudo и конфигурационный файл /etc/sudoers, администраторам, т.е. пользователям с UID root, разрешено передавать часть или все свои полномочия другим пользователям.

Файл sudoers должен редактироваться только командой visudo, которая блокирует файл и осуществит проверку грамматики. Это обязательно во избежание возникновения ошибок в синтаксисе sudoers, так как sudo не будет работать при наличии ошибок в sudoers.

Формат файла /etc/sudoers прост: начинается с четырех опциональных секций, и заканчивается присвоением специальных прав. Файл может включать пустые строки, строки комментариев, которые начинаются со значка #. Опциональные (необязательные) секции следующие:

- User Alias (Псевдоним пользователя). Присваивает псевдоним одному пользователю или группе пользователей. Пользователь может иметь несколько псевдонимов.
- "Run as" Alias ("Работает как" Псевдоним). Определяет, вместо кого именно пользователь команды sudo будет работать. По умолчанию sudo подразумевает суперпользователя root, но есть возможность работать вместо кого-либо другого.
- Host Alias (Псевдоним рабочей станции). Определяет, каким рабочим станциям присваиваются права.
- Command Alias (Псевдоним Команды). Определяет псевдоним для той или иной команды.

Использование псевдонимов не обязательно, но они сильно облегчают дальнейшее редактирование файла. Например, если вы хотите наделить пользователя user1 правами, которые имеет user2, нужно добавить первого в группу последнего и вам не придется тратить много времени, переписывая одинаковые строки. Существует специальный псевдоним ALL ("ВСЕ"), и он может означать "ВСЕ" пользователи, "ВСЕ" хосты и т.д.

Для определения псевдонимов пользователя нужно использовать конструкцию User_Alias <ПСЕВДОНИМ> = <имя пользователя 1>, <имя пользователя 2**>, <...>**. Например:

User_Alias FULLTIMERS = fullt1, fullt2, fullt3

User_Alias USERS = user1, user2, user3

User_Alias SYSTEMS = root, operator7, sysadm

Для определения псевдонимов Runas (Выполнить как) нужно использовать конструкцию Runas_Alias <ПСЕВДОНИМ> = <имя пользователя 1>, <имя пользователя 2>, <...>. Например:

Runas_Alias OP = root, operator

Runas_Alias DB = oracle, Sybase

Для определения псевдонимов вычислительныхмашин нужно использовать конструкцию Host_Alias <ПСЕВДОНИМ> = <рабочая станция 1>, <рабочая станция 2**>, <...>**. Например:

```
Host_Alias    SPARC = bigtime, eclipse, moet, anchor :\
                  SGI = grolsch, dandelion, black :\
                  ALPHA = widget, thalamus, foobar :\
                  HPPA = boa, nag, python
Host_Alias    CUNETS = 128.138.0.0/255.255.0.0
Host_Alias    CSNETS = 128.138.243.0, 128.138.204.0/24, 128.138.242.0
Host_Alias    SERVERS = master, mail, www, ns
Host_Alias    CDROM = orion, perseus, hercules
```

Для определения псевдонимов Cmnd (команд) нужно использовать конструкцию Cmnd_Alias <ПСЕВДОНИМ> = <путь к исполняемой команде 1>, <путь к исполняемой команде 2>, <...>. Например:

```
Cmnd_Alias    DUMPS = /usr/bin/mt, /usr/sbin/dump, /usr/sbin/rdump,\
                  /usr/sbin/restore, /usr/sbin/rrestore
Cmnd_Alias    KILL = /usr/bin/kill
Cmnd_Alias    PRINTING = /usr/sbin/lpc, /usr/bin/lprm
Cmnd_Alias    SHUTDOWN = /usr/sbin/shutdown
Cmnd_Alias    HALT = /usr/sbin/halt, /usr/sbin/fasthalt
Cmnd_Alias    REBOOT = /usr/sbin/reboot, /usr/sbin/fastboot
Cmnd_Alias    SHELLS = /usr/bin/sh, /usr/bin/csh, /usr/bin/ksh, \
                  /usr/local/bin/tcsh, /usr/bin/rsh, \
                  /usr/local/bin/zsh
Cmnd_Alias    SU = /usr/bin/su
```

Чтобы настроить для пользователя все права пользователя root при выполнении команды sudo, нужно добавить в файл конструкцию <имя_пользователя> ALL=(ALL) ALL в секции "User privilege specification". Добавим полномочия администратора пользователю user:

```
user ALL=(ALL) ALL
```

Чтобы настроить root-привилегии всем членам группы, нужно использовать конструкцию %<имя_группы> ALL=(ALL) ALL. Добавим root-привилегии всем членам группы system:

```
%system ALL=(ALL) ALL
```

Чтобы дать пользователю права на выполнение от root конкретных команд, нужно использовать конструкцию **<**имя пользователя> ALL = <путь к исполняемому файлу команды>, <путь к исполняемому файлу команды 2**>, <...>**. Добавим пользователю user права на выполнение от имени root выполнения команд mount и kill следующим образом:

user ALL = /bin/mount, /bin/kill

Чтобы дать возможность пользователю ("пользователь 1") выполнять команды от имени другого пользователя ("пользователь 2", "пользователь 3" и.т.д.), необходимо добавить конструкцию **<**пользователь 1> ALL = (<пользователь 2>, <пользователь 3>, <...>) <путь к исполняемому файлу команды 1>, <путь к исполняемому файлу команды 2>, **<...>**. Например, для того чтобы добавить право выполнить команду ark от имени пользователей user2 и user3, пользователю user нужно добавить в файл строку:

user ALL = (user2, user3) /usr/bin/ark

Теперь пользователь user может выполнить команду ark от имени user2 или user3 при помощи ключа u, набрав в консоли:

sudo -u user2 ark

Добавим право выполнить команду ark от имени пользователей user2 и user3 пользователям fullt1, fullt2 и fullt3, определенных под псевдонимом FULLTIMERS**,** для этого нужно добавить в файл строку:

FULLTIMERS ALL = (user2, user3) /usr/bin/ark

Чтобы добавить пользователю user2 возможность выполнять любую команду на машинах с псевдонимом CSNETS (сети 128.138.243.0, 128.138.204.0 и 128.138.242.0), нужно добавить строку:

user2 CSNETS = ALL

Добавить пользователю operator возможность выполнять команды, ограничивающиеся простым обслуживанием (в данном примере таковыми будут резервное копирование, уничтожение процессов, система печати, выключение системы и любая команда в каталоге /usr/oper/bin/), можно следующими строками:

operator ALL = DUMPS, KILL, PRINTING, SHUTDOWN, HALT, REBOOT,\

/usr/oper/bin/

Чтобы добавить пользователю user2 возможность выполнить любую команду на любой машине, за исключением машин в Host_Alias SERVERS (master, mail, www и ns), нужно вставить строку:

user2 ALL, !SERVERS = ALL

Чтобы пользователь user мог выполнять любую команду в каталоге /usr/local/op_commands/ на рабочих станциях CSNETS, но только как пользователь operator, нужно добавить в файл строку:

user CSNETS = (operator) /usr/local/op_commands/

Чтобы любой пользователь мог монтировать или размонтировать CD-ROM на машинах в Host_Alias CDROM (orion, perseus, hercules) без ввода пароля, нужно добавить строки:

ALL CDROM = NOPASSWD: /sbin/umount /CDROM,\

/sbin/mount -o nosuid\,nodev /dev/cd0a /CDROM

По умолчанию sudo запоминает пароли на 5 минут. Чтобы установить для пользователя или группы отдельное правило, нужно добавить конструкцию Defaults:<имя_объекта> timestamp_timeout=<время запоминания>. Например, чтобы пароль пользователя user не запоминался вообще, нужно добаить строку:

Defaults:user timestamp_timeout=0

Для того чтобы пароль пользователя user запоминался на все время аптайма, нужно добавить:

Defaults:user timestamp_timeout=-1

Чтобы пользователь мог выполнять sudo без паролей, нужно добавить <имя пользователя> = NOPASSWD: <путь к исполняемому файлу команды 1>, <путь к исполняемому файлу команды 2>, <...>. Впишем следующую строку, которая даст возможность пользователю user использовать команду kill без запроса пароля:

user = NOPASSWD: /bin/kill

Для того чтобы пользователь мог никогда не вводить пароль для выполнения команд от имени root, нужно добавлять **<**имя пользователя> ALL=(ALL) NOPASSWD: ALL.

Например:

user ALL=(ALL) NOPASSWD: ALL

4.8 Библиотеки PAM

МСВСфера 6.3 АРМ использует комплект библиотек "Pluggale Authentication Modules" (PAM). Достоинство PAM заключается в модульности, благодаря которой можно легко изменить используемый метод аутентификации путём редактирования конфигурационного файла, находящегося в каталоге /etc/pam.d.

PAM предоставляет четыре четко определенные зоны безопасности, хотя не все они могут понадобиться вашим приложениям:

- account определяет ограничения прав учетных записей;
- auth выполняет идентификацию пользователя;
- password работает исключительно с функциями обработки паролей, такими как ввод нового пароля;
- session управляет подключением, включая вход в систему.

Для каждого приложения, которое будет использовать PAM, нужно создать отдельный конфигурационный файл в директории /etc/pam.d, причем имя этого файла должно совпадать с именем приложения. Например, конфигурационный файл для команды login будет иметь имя /etc/pam.d/login.

Затем нужно определить, какие модули будут применяться, создав для этого "стек" операций. PAM исполняет все модули соответствующего стека и, в зависимости от результата их работы, подтверждает или отклоняет запрос пользователя. Также нужно определить, являются ли проверки обязательными. Файл "other" должен содержать стандартные правила для всех приложений, не требующих специальных правил.

Модули optional могут давать успешный или неуспешный результат. В зависимости от результата работы такого модуля PAM возвращает значение "success" (успех) или "failure" (неудача).

Модули required являются обязательными. В случае неудачи PAM возвращает значение "failure", но только после исполнения всех остальных модулей этого стека.

Модули requisite тоже должны успешно завершить работу. Но если они потерпели неудачу, PAM возвращает значение "failure", не исполняя другие модули.

В случае удачного завершения работы модулей sufficient PAM немедленно возвращает значение "success", не исполняя другие модули.

Структура конфигурационного файла проста. В него можно включать комментарии, начинающиеся с символа #. Длинные строки можно разбивать, добавляя обратную косую черту (\). Строки файла содержат три поля: область (account, auth, password или session), управляющий флажок (optional, required, requisite или sufficient), путь к модулю, который надо исполнить, и всевозможные параметры. Можно подключать правила из других файлов командой include, например, auth include common-account.

Вывод информации пользователю при авторизации

о дате и времени последнего входа пользователя в систему

Чтобы настроить вывод информации пользователю при авторизации о дате и времени последнего входа в систему, нужно добавить в файл /etc/pam.d/system-auth строку session optional pam_lastlog.so, как показано на рис. 87.

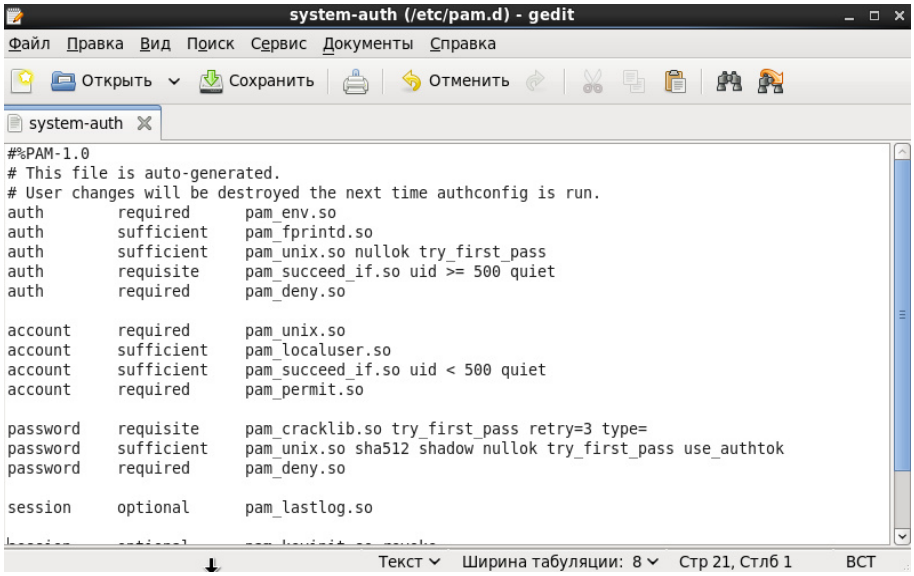


Рисунок 87 - Редактирование файла system-auth

В результате при авторизации пользователь получит информацию о дате и времени последнего входа в систему (рис. 88).

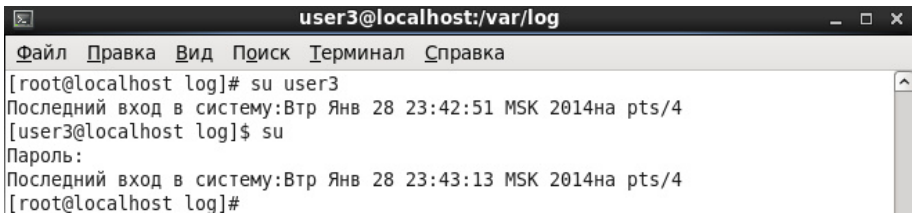


Рисунок 88 - Вывод даты и времени последнего входа в систему

Для вывода обобщенной информации о последних входах пользователей в систему root может использовать команду lastlog в консоли (рис. 89).

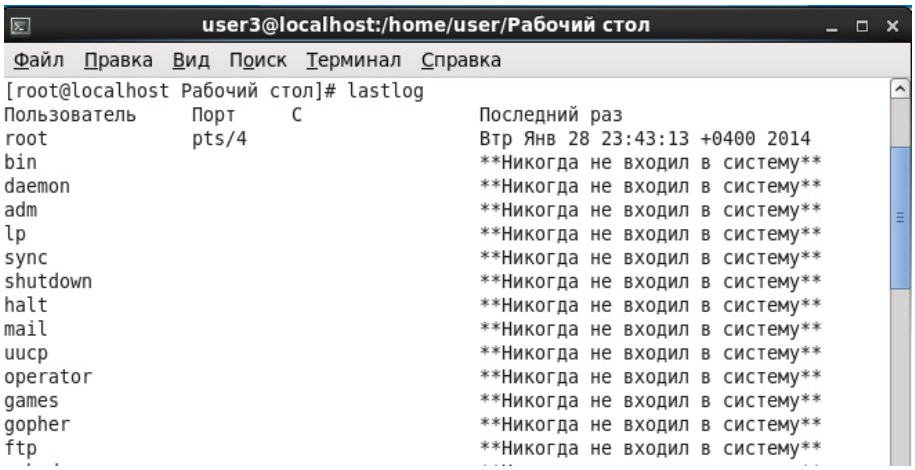


Рисунок 89 - Выполнение команды lastlog

Блокировка учетной записи пользователя

после нескольких неудачных попыток ввода пароля

Чтобы повысить безопасность системы, можно блокировать логин пользователя после нескольких неудачных попыток ввода пароля. Учетная запись может быть заблокирована на некоторый промежуток времени или до тех пор, пока root не разблокирует пользователя вручную.

Для блокировки учетной записи пользователя, который совершит определенное количество неудачных попыток входа, используется модуль PAM pam_tally2, который можно подключить на любом этапе входа в систему.

Чтобы заблокировать учетную запись пользователя на определенное время, после определенного количества неудачных попыток ввода, нужно изменить файл /etc/pam.d/system-auth.

Допишем в секцию auth следующую строку:

auth required pam_tally2.so deny=2 onerr=fail unlock_time=60

Значение unlock_time - это время в секундах, на которое пользователь будет заблокирован после двух (значение параметра "deny") неудачных попыток входа.

В том же файле в начало секции account нужно добавить:

account required pam_tally2.so

Если в файле /etc/pam.d/system-auth есть строчки вида:

auth requisite pam_succeed_if.so uid >= 500 quiet

auth required pam_deny.so

то их надо удалить или закомментировать.

Строку auth sufficient pam_unix.so nullok try_first_pass нужно заменить на:

auth required pam_unix.so nullok try_first_pass

В результате должен получиться файл, похожий по структуре на файл на рис. 90.

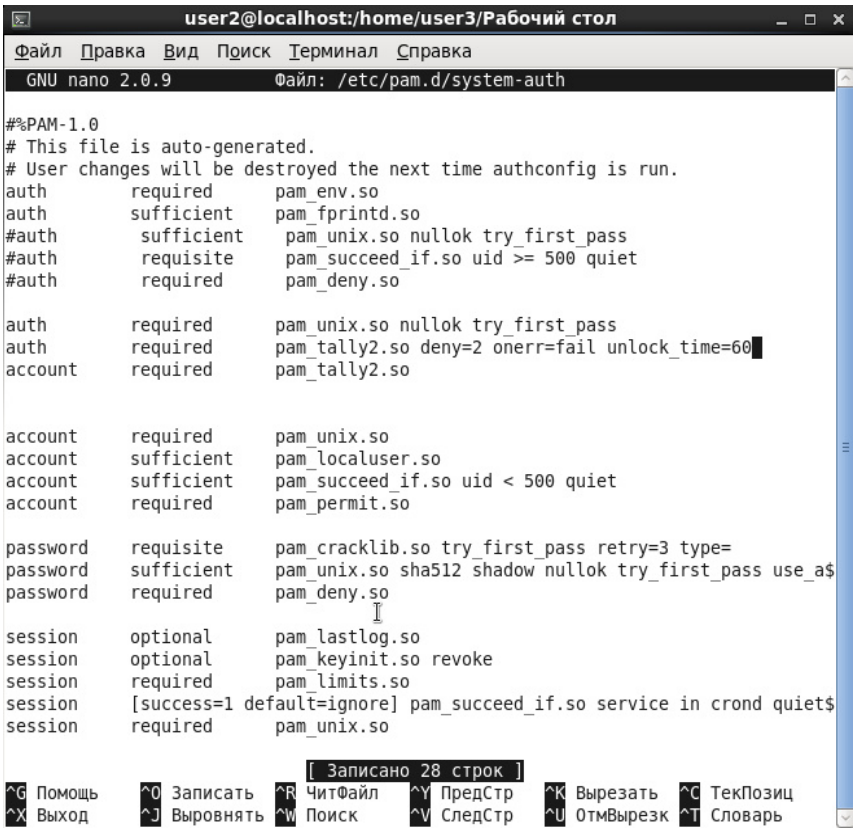


Рисунок 90 - Файл /etc/pam.d/system-auth

Пользователь, допустивший подряд две неверных попытки входа, на третьей получит сообщение о том, что его учетная запись заблокирована, доступ к учетной записи он получит через минуту (установленное время в параметр unlock_time), как на рис. 91.

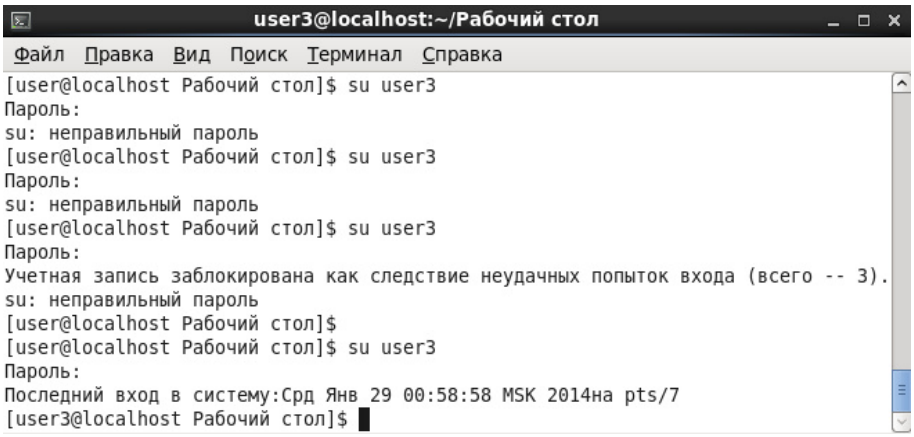


Рисунок 91 - Результат временной блокировки учетной записи пользователя

Пользователь с правами root может просмотреть отчет о попытках аутентификации, находящийся в /var/log/secure (рис. 92).

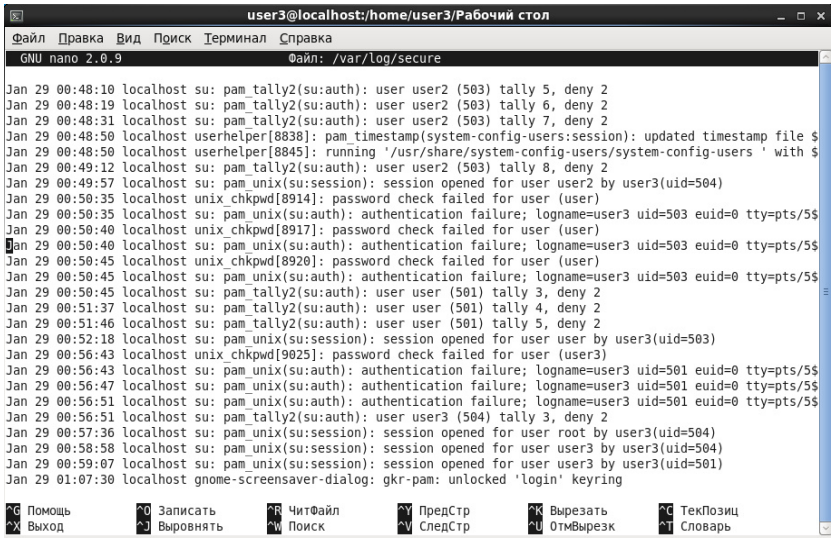


Рисунок 92 - Отчет о попытках аутентификации

Чтобы просмотреть заблокированных пользователей администратору с правами root, нужно ввести команду pam_tally2 (рис. 93).

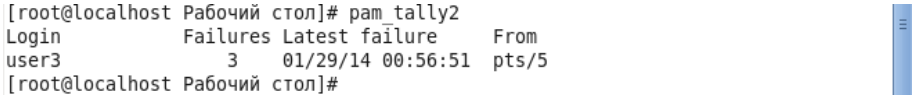


Рисунок 93 - Отчет о заблокированных пользователях

Если удалить параметр unlock_time и его значение (рис. 94), то заблокированный пользователь не сможет авторизоваться, пока его не разблокирует root (рис. 95).

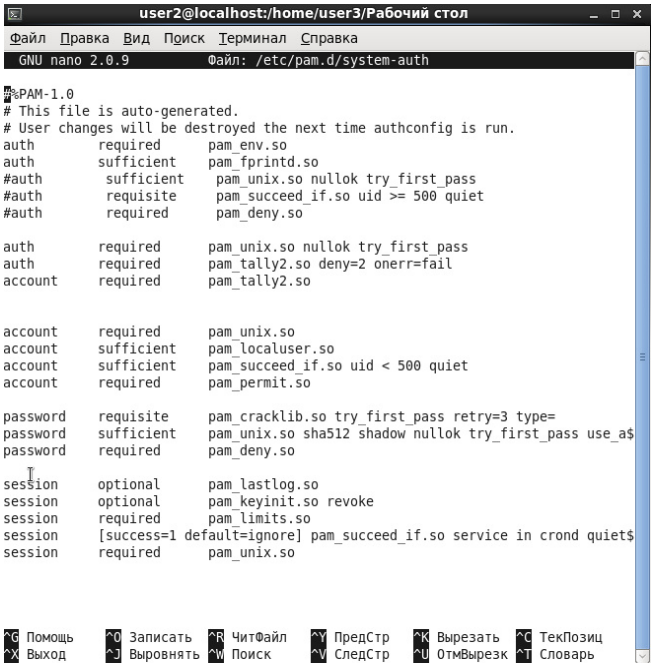


Рисунок 94 - Файл /etc/pam.d/system-auth без параметра unlock_time

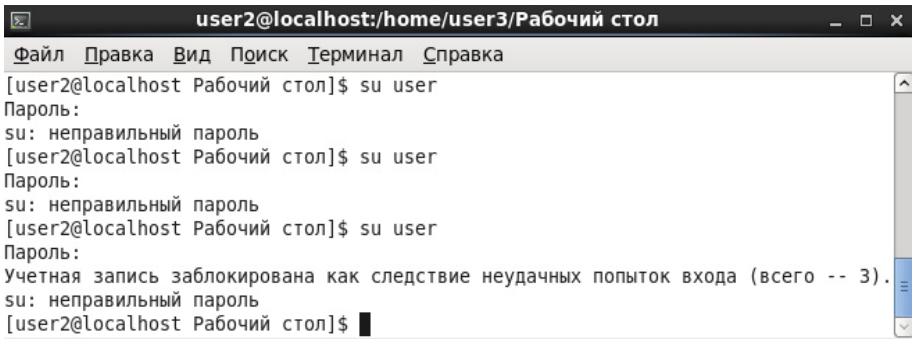


Рисунок 95 - Блокировка пользователя после неудачных попыток авторизации

Разблокировать пользователя можно с правами root с помощью команды pam_tally2 -u <имя пользователя> -r, как на рис. 96.

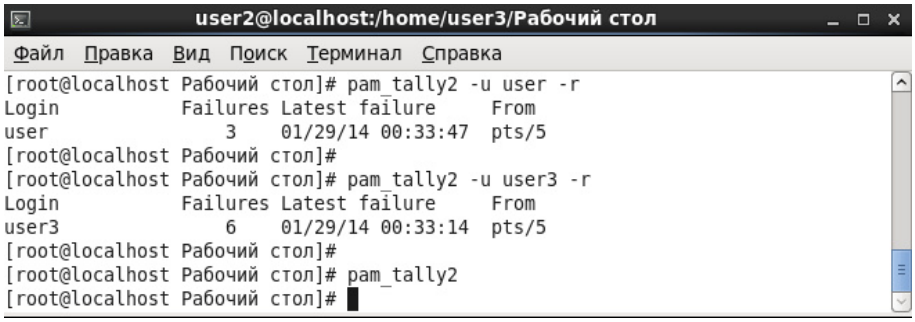


Рисунок 96 - Разблокировка пользователей

4.9 Приложение "Хранитель экрана"

По умолчанию для пользователя время бездействия ограничено утилитой «Хранитель экрана» (меню "Система", пункт меню "Параметры"). Времени бездействия по умолчанию ограничено до 5 минут (рис. 97).

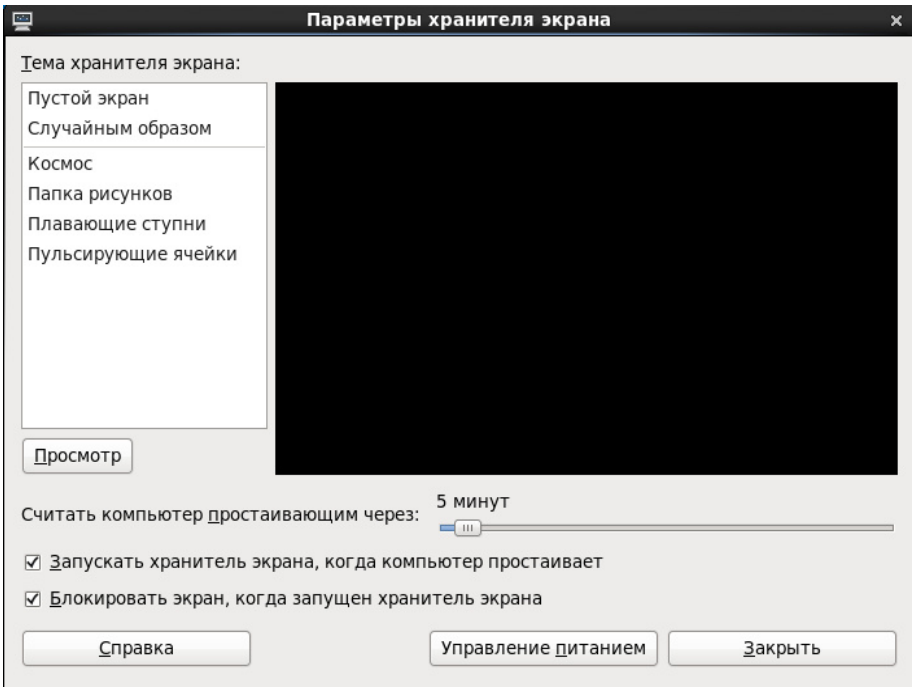


Рисунок 97 - Время бездействия, установленное по умолчанию

После истечения интервала времени бездействия пользователя будут очищены и перезаписаны устройства отображения, а также заблокированы любые действия по доступу к данным пользователя или устройствам отображения, кроме необходимых для разблокирования сеанса (рис. 98). Для разблокирования сеанса будет необходима повторная авторизация.

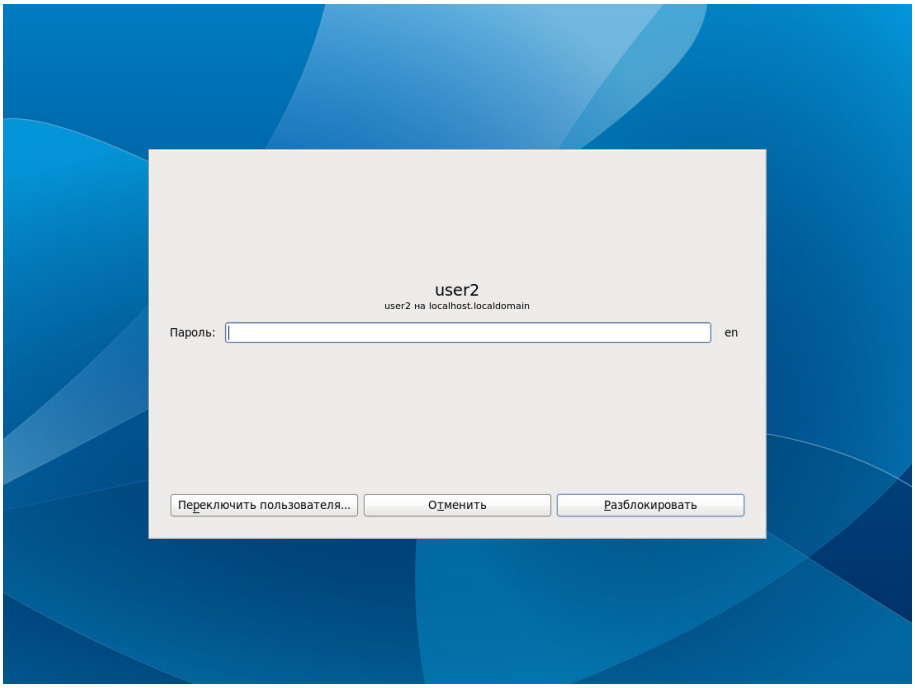


Рисунок 98 - Блокировка сеанса пользователя после истечения времени бездействия

Пользователь может самостоятельно устанавливать временной интервал для блокировки интерактивного сеанса в приложении "Хранитель экрана", задав время, после которого считать компьютер простаивающим, и выбрав блокировку экрана, когда запущен хранитель экрана (рис. 97).

В результате выполненных действий после простоя компьютера, пользователь обратится к своему сеансу, но не получит доступ к данным без повторной аутентификации для разблокировки сеанса (рис. 98).

4.10 Подсистема ядра RFKill

Многие современные компьютеры оборудованы устройствами WiFi, Bluetooth и 3G. Подсистема ядра под названием RFKill предоставляет интерфейс для управления подобного рода устройствами. Отключаемые устройства могут быть переведены в состояние, из которого

их можно будет позднее повторно активировать (временное блокирование) или нельзя активировать (постоянное блокирование).

RFKill включает интерфейс API, с помощью которого драйверы ядра, отвечающие за работу RFKill, могут осуществлять регистрацию в ядре. Эти драйверы позволяют включать и отключать устройства, опрашивать их состояние и уведомлять пользовательские программы.

Интерфейс RFKill определен в файле /dev/rfkill, который содержит текущее состояние всех встроенных устройств передачи. Состояние RFKill каждого устройства зарегистрировано в sysfs.

При изменении состояния устройства RFKill генерирует событие.

Выполните команду rfkill list для получения списка устройств и их индексов, начиная с нуля. Индекс можно использовать для блокирования устройств. Например:

rfkill block 0

Эта команда заблокирует первое устройство.

Можно заблокировать отдельные категории устройств. Например:

rfkill block wifi

Эта команда заблокирует все устройства WiFi. Чтобы полностью заблокировать все устройства в системе, выполните rfkill block all.

Команда rfkill unblock <группа устройств или номер устройства> разблокирует устройства. Полный список параметров можно просмотреть с помощью команды rfkill help (рис. 99).

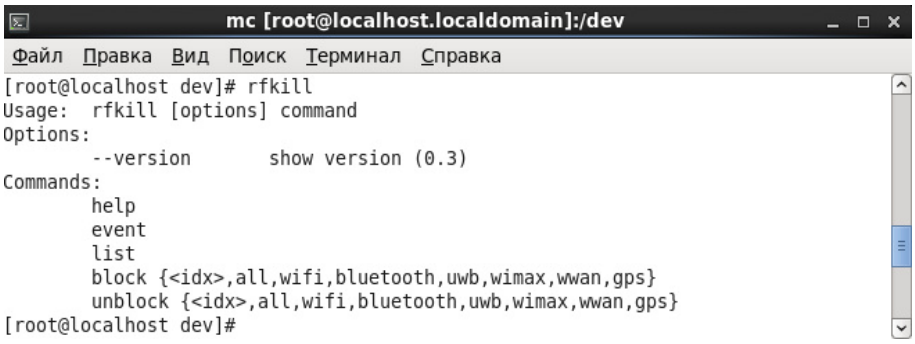


Рисунок 99 - Параметры команды rfkill

4.11 Приложение "Настройка Kickstart"

Для обеспечения доверенной загрузки системы используется приложение "Настройка Kickstart", которое вызывается из меню "Приложения->Системные->Kickstart".

На вкладке "Метод установки" (рис. 100) приложение позволяет выбрать между выполнением новой установки и обновлением текущей системы в качестве метода установки, а также задать установочный носитель (среди вариантов CD-ROM, NFS, FTP, HTTP, жесткий диск).

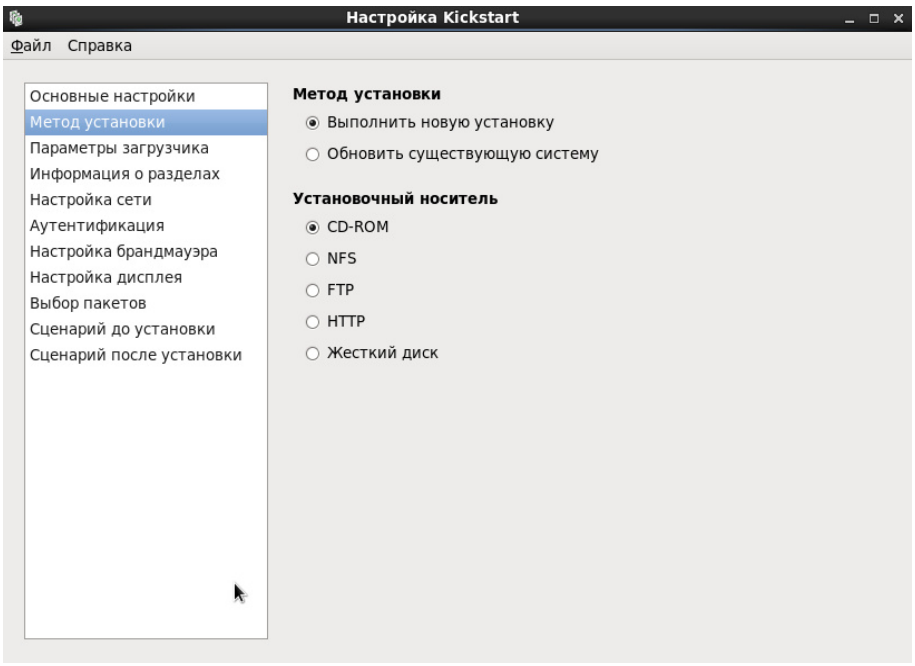


Рисунок 100 - Вкладка "Метод установки" приложения "Настройка Kickstart"

На вкладке "Параметры загрузчика" для обеспечения безопасности от несанкционированной загрузки нештатной ОС можно защитить загрузку через GRUB, установив пароль для GRUB и зашифровав его, как показано на рис. 101. Если вы решили зашифровать пароль, то при сохранении файла он будет зашифрован и записан в файл kickstart. Если вы вводите уже зашифрованный пароль, снимите этот флажок.

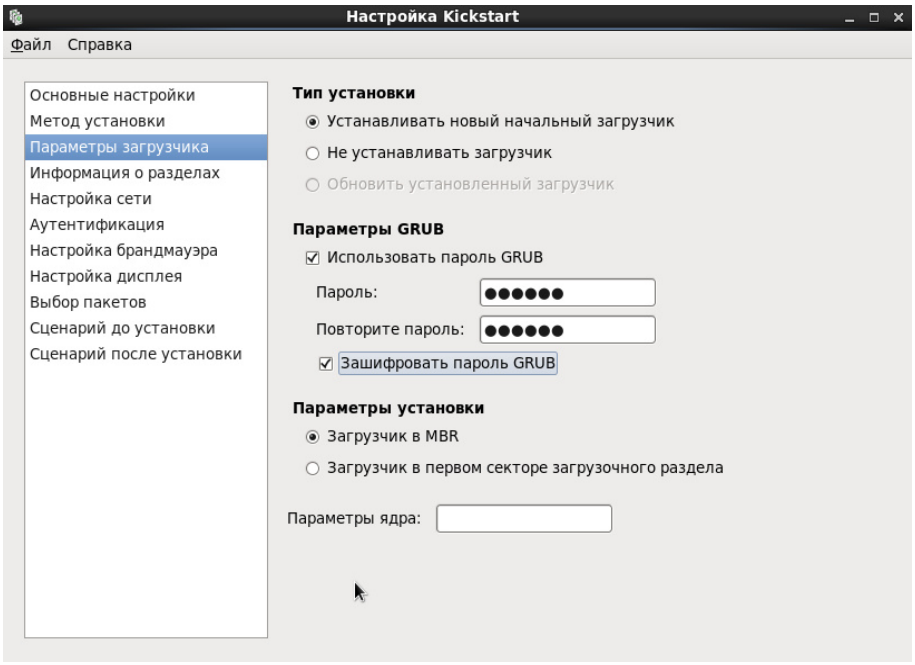


Рисунок 101 - Вкладка "Параметры загрузчика" приложения "Настройка Kickstart"

При следующей загрузке системы меню GRUB не даст вам вызвать редактор или командную строку, если вы не нажмёте сначала [p] и не введёте затем пароль GRUB.

Но если на компьютере окажется несколько операционных систем, подобные меры безопасности не запретят загрузить небезопасную операционную систему. Для исправления подобных ошибок нужно внести изменения в конфигурационный файл /boot/grub/grub.conf.

Прямо под строкой title с небезопасной операционной системой нужно добавить строку lock. Например, для системы Windows будет выглядеть так:

title Windows

lock

Чтобы задать для конкретного ядра или другой системы отдельный пароль, после строки lock добавьте строку с паролем. Например:

title Windows

lock

password --md5 <password-hash>

Так же необходимо поставить пароль на BIOS. У разных производителей BIOS эта установка отличается друг от друга, поэтому подробное описание здесь не приводится.

Пароли BIOS не дадут злоумышленникам загрузить систему и помешают утечке информации, но злоумышленник может извлечь жёсткий диск, вставить его в другой компьютер без ограничений BIOS, и, обратившись к жёсткому диску, прочитать его содержимое. В таких случаях рекомендуется использовать компьютеры, ограничивающие доступ к внутреннему оборудованию с помощью специальных защитных и/или опечатывающих устройств.

4.12 Файл /etc/issue

Для предупреждения пользователя при входе в систему о том, что в ней реализованы меры защиты информации и о необходимости соблюдения установленных правил обработки информации (или вывода другой важной информации), используется файл /etc/issue.

Традиционно в этом файле присутствует информация об операционной системе и ядре. Администратор может добавить в файл необходимую информацию, например, как на рис. 102.

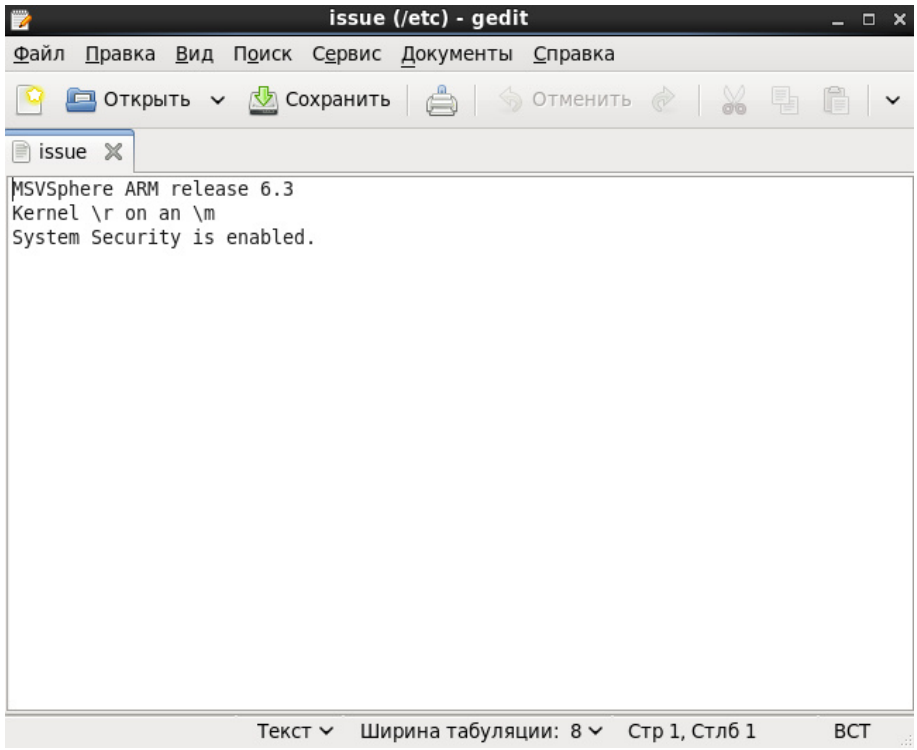


Рисунок 102 - Редактирование файла /etc/issue

После перезагрузки в текстовом режиме на экран будет выдаваться приглашение входа в систему вместе с предупреждением, добавленным администратором (рис. 103).

Рисунок 103 - Приглашение входа в систему

Файл /etc/issue является простым текстовым файлом, в котором можно записать определенные последовательности управляющих символов для того, чтобы можно было отображать системную информацию. Все управляющие последовательности, указываемые в файле issue, состоят из обратного слеша ("\"), за которым идет один их символов, приведенный ниже (так "\d", присутствующий в файле /etc/issue, будет вставлять текущую дату).

b вставка текущей скорости линии;

d вставка текущей даты;

s вставка названия системы, имени операционной системы;

l вставка названия текущего терминала;

m вставка идентификатора архитектуры системы, например, i686;

n вставка имени узла, которым является машина, также известным как имя хоста;

o вставка доменного имени машины;

r вставка номера релиза ядра, например, 2.6.11.12;

t вставка текущего времени;

u вставка количества пользователей, зарегистрированных в системе в текущий момент;

U вставка строки "1 user" или " users", где - количество пользователей зарегистрированных в текущий момент;

v вставка версии ОС, например, даты сборки и так далее.

Чтобы отобразить подобную информацию при дистанционном входе в систему, нужно использовать файл issue.net. Но ssh будет использовать этот файл только в том случае, если в конфигурационном файле будет указан соответствующий параметр, причем управляющие последовательности интерпретироваться не будут.

4.13 Метки безопасности

МСВСфера 6.3 АРМ обеспечивает автоматизированный контроль связи атрибутов безопасности (меток безопасности) с информацией. Эти метки автоматически присваиваются процессам и объектам. Такая политика осуществляется модулем безопасности SELinux.

Только авторизованные администраторы могут установить и изменить любые метки, присвоенные объектам или субъектам. Поэтому контроль доступа не зависит от пользователя как в случае с DAC.

Система поддерживает и сохраняет атрибуты безопасности, связанные с информацией в процессе ее хранения и обработки. Атрибуты безопасности субъектов и объектов, также называемые контекстом защиты, имеют определённый формат. Контекст защиты является строкой ASCII. С целью увеличения производительности, ядро во время выполнения преобразовывает строку в 32-разрядное целое число.

Контекст защиты состоит из четырёх разделенных двоеточием компонентов. Они соответствуют пользователю, роли, типу и диапазону MLS для субъеков или объектов.

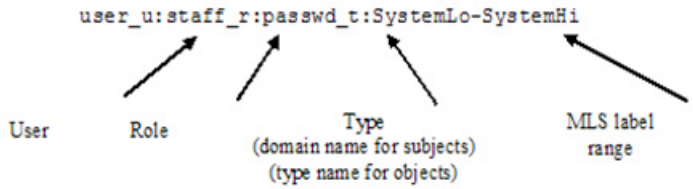


Рисунок 104 - Компоненты контекста защиты

- Пользователь (User): компонентом пользователя является имя пользователя SELinux.
- Роль (Role): компонентом роли является роль SELinux, соответствующая субъекту или объекту. Для субъектов роль используется для доступа к домену. Для объектов компонент роли не используется и соответствует object_r.
- Тип (Type): поле типа представляет собой домен субъекта или тип объекта. Домены и типы эквивалентны классам для процессов и ресурсов соответственно. Решения о предоставлении доступа в ядре основываются на домене субъекта и

типе объекта.

- Диапазон меток MLS (MLS label range): диапазон меток MLS содержит две метки MLS. Менее значимая метка располагается слева, более значимая метка – справа. Метки разделены тире и формируют диапазон меток. Менее значимая метка соответствует разрешению действительной MLS метке субъекта. Более значимая метка соответствует разрешению для субъекта. Разрешение субъекта соответствует разрешению пользователя, от имени которого действует субъект. Для объектов, таких как обычные файлы, политика безопасности устанавливает обе метки равными. Таким образом, объекту действительно соответствует единственный уровень. Объекты, такие как каталоги, устройства и сокеты могут иметь более значимую метку, отличную от менее значимой. Такие объекты являются многоуровневыми, и их диапазон MLS меток требует, чтобы уровень чувствительности любой информации, проходящей через них, доминировал над менее значимой меткой и был охвачен более значимой меткой.

Каждая MLS метка состоит из двух компонент: иерархический уровень классификации (или уровень чувствительности) и неиерархический набор категорий.

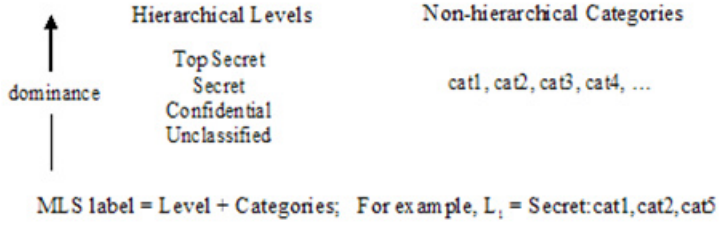


Рисунок 105 - Компоненты контекста защиты

Между любыми двумя MLS метками могут существовать четыре следующих отношения:

- L1 равен L2 (уровни равны, наборы категорий эквивалентны),
- L1 доминирует над L2 (уровень L1> = уровню L2, набор категорий L2 равен или является подмножеством набора категории L1),
- L2 доминирует над L1 (уровень L2> = уровню L1, набор категорий L1 равен или является подмножеством набора категорий L2),
- L1 несравним с L2 (L1 и L2 не равны, и ни один не доминирует над другим),

Например, если L1 = Secret:cat1, cat2, cat5, L2 = Confidential:cat1, cat2, и L3 = Unclassified:cat1, cat5, то

- L1 доминирует над L2
- L2 во власти L1
- L2 несравним с L3

Хранение атрибутов. Атрибуты SELinux хранятся в структуре процесса task_struct для субъектов, а для объектов в дисковом inode в файловой системе ядра. Они хранятся в структуре kern_ipc_perm для IPC объектов SystemV, в структуре sock для сокетов и в структуре xfrm_state для netlink сокетов. SELinux отображает недопустимые контексты на контекст system_u:object_r:unlabeled_t:s0.

Чтобы пользователи имели возможность использовать метки безопасности, нужно настроить систему MLS. Откроем конфигурационный файл /etc/selinux/config в редакторе nano и выставим атрибуты SELINUXTYPE=mls и SELINUX=permissive (рис. 106).

Рисунок 106 - Редактирование файла /etc/selinux/config

При следующей загрузке системы SELinux произведет реиндексацию всех файлов в системе (добавит метки чувствительности s0-s15). Выполним для перезагрузки команду:

reboot

Повторно отредактируем файл /etc/selinux/config, выставим SELINUX в enforcing, как на рис. 107.

Рисунок 107 - Повторное редактирование файла /etc/selinux/config

Выполним для перезагрузки системы команду:

reboot

Проверим статус selinux в системе с помощью команд (рис. 108):

getenforce

sestatus

Рисунок 108 - Проверка статуса selinux

Режим Selinux MLS расширяет атрибуты файлов 16-ю метками чувствительности. Чтобы проверить, предоставляет ли система в данный момент эту возможность, введем команду в консоли (рис. 109):

seinfo

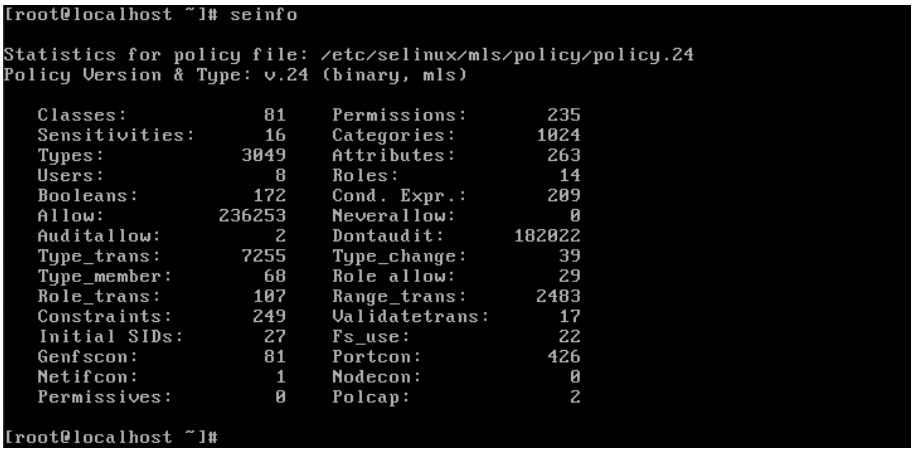


Рисунок 109 - Проверка предоставляемых меток чувствительности при SELINUX=enforcing

Как видно на рис. 109 значение переменной Sensitivities — 16. Это означает, что в данный момент режим Selinux MLS расширяет атрибуты файлов 16-ю метками чувствительности.

Для сравнения при включенной политике по умолчанию (targeted) доступна только одна метка чувствительности (рис. 110):

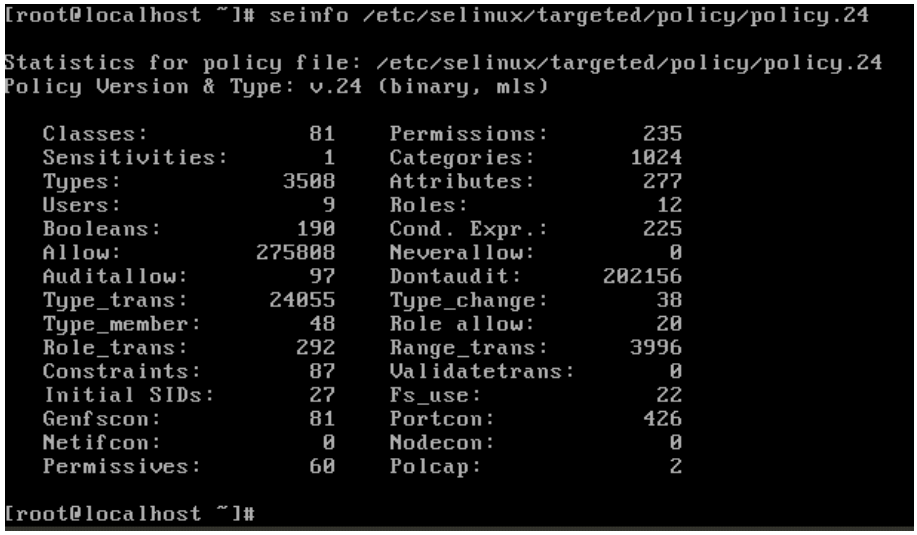


Рисунок 110 - Проверка предоставляемых меток чувствительности при SELINUX=targeted

Диапазон значений категорий в обоих режимах можно задавать от 1 до 1024. Просмотреть MLS таблицу преобразований для SELinux можно, открыв фйл /etc selinux/mls/setrans.conf (рис. 111).

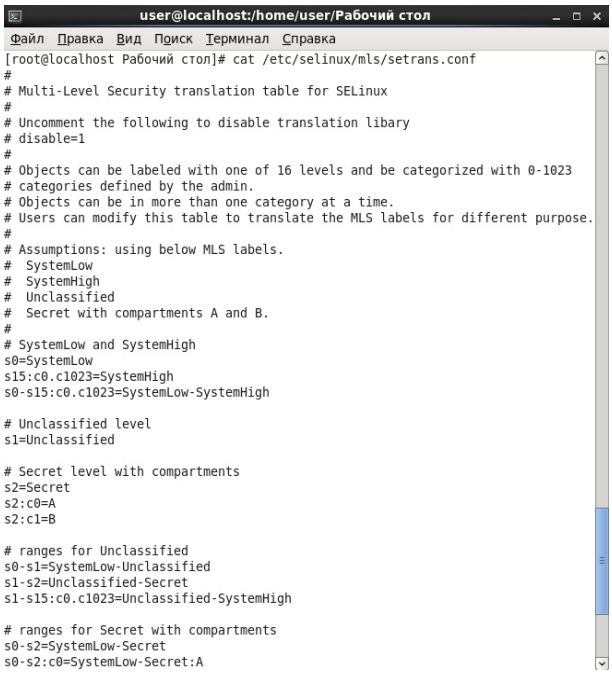


Рисунок 111 - Конфигурационный файл /etc selinux/mls/setrans.conf

В МСВСфера 6.3 АРМ обеспечивается возможность отображения пользователям в удобном для чтения виде меток безопасности для каждого из объектов доступа. Для этого пользователю нужно выполнить команду id -Z (рис. 112).

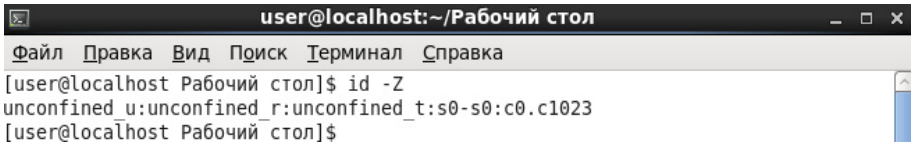


Рисунок 112 - Метки безопасности пользователя

Файлы и папки тоже имеют контекст безопасности. Чтобы его просмотреть, нужно выполнить команду ls -Z <имя_файла> или ls -Z для просмотра контекстов безопасности всех файлов в папке. Создадим тестовый файл testfile от обычного пользователя и посмотрим его контекст безопасности, как на рис. 113.

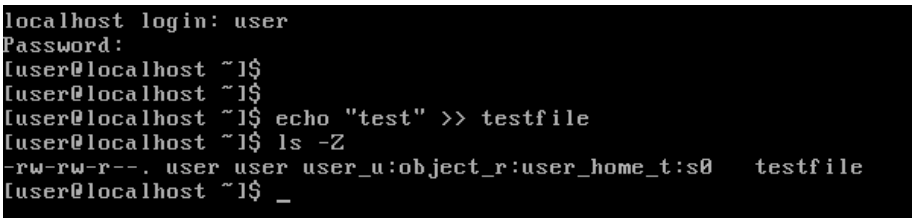


Рисунок 113 - Создание и просмотр атрибутов файла testfile

Изменить метку чувствительности пользователя или файла (группы файлов) с полномочиями администратора можно в приложении "Администрирование SELinux" на вкладках "Присвоение меток файлам" и "Пользователь SELinux", как описано в подразделе 4.6.

5 УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ

5.1 Основные сведения

Средства управления безопасностью МСВСфера 6.3 АРМ предоставляют следующие возможности:

- обеспечение контроля доступа, основанного на ролях;
- поддержка активных и дополнительных ролей в SELinux;
- ограничение доступа с помощью политики RBAC;
- поддержка привилегий для выполнения административных действий над данными;
- поддержка привилегий для функционала обеспечения доступа в пространстве пользователя и ядра;
- поддержка системных вызовов файловой системы, использующихся для установки атрибутов безопасности объектам с целью настройки контроля доступа;
- управление базами данных аутентификации;
- управление настройками аудита;
- управление контролем целостности системы;
- использование аппаратных часов для поддержки надежных меток времени.

Вышеперечисленные возможности управления безопасностью реализуются с помощью следующих программных компонент:

- утилита chage;
- утилита chfn;
- утилита chsh;
- утилита useradd;
- утилита usermod;
- утилита userdel;
- утилита groupadd;
- утилита groupmod;
- утилита groupdel;
- утилита chcat;
- утилита chcon;
- утилита checkpolicy;

- утилита load_policy;
- утилита restorecon;
- утилита restorecond;
- утилита semodule;
- утилита setenforce;
- утилита setfiles;
- утилита AIDE;
- утилита AMTU;
- утилита sudo;
- утилита getfacl;
- утилита setfacl;
- утилита hwclock;
- утилита rnano;
- приложение «Администрирование Selinux»;
- конфигурационные файлы;
- приложение «Менеджер пользователей»;
- средства управления аудитом;
- приложение «Дата и время».

5.2 Утилита chage

Команда chage изменяет настройки срока действия пароля, т. е. изменяет количество дней между сменой пароля и датой последнего изменения пароля. Информация используется системой для определения времени, когда пользователь должен сменить свой пароль.

Командой chage может пользоваться только суперпользователь, за исключением использования ее с параметром "-l", который позволяет непривилегированным пользователям определить время, когда истекает их пароль или учетная запись.

Команда chage поддерживает следующий набор опций:

-m — изменяется значение mindays на минимальное число дней между сменой пароля. Значение 0 в этом поле обозначает, что пользователь может изменять свой пароль, когда угодно.

-M — изменяется значение maxdays на максимальное число дней, в течение которых пароль еще действителен. Когда сумма maxdays и lastday меньше, чем текущий день, у пользователя будет запрошен новый пароль до начала работы в системе.

-d — изменяется значение lastday на день, когда был изменен пароль последний раз (число дней с 1 января 1970). Дата также может быть указана в формате ГГГГ-ММ-ДД или в другом формате.

-E — используется для задания даты, с которой учетная запись пользователя станет недоступной.

-I — используется для задания количества дней "неактивности", то есть дней, когда пользователь вообще не входил в систему, после которых его учетаня запись будет заблокирована. Значение 0 отключает этот режим.

-W — используется для задания числа дней, когда пользователю начнет выводиться предупреждение об истечении срока действия его пароля и необходимости его изменения.

Все значения хранятся в виде дней, если используется система теневых паролей, но если используется системы обычных паролей, то значения преобразуются в недели.

Если параметры не указаны, то chage работает в интерактивном режиме, сообщая пользователю текущие значения полей. Необходимо далее либо ввести новое значение поля, либо оставить его как есть. Текущее значение поля показывается в скобках [ ].

Информация об учетной записи пользователя находится в /etc/passwd.

Информация о теневой учетной записи пользователя находится в /etc/shadow.

Например, чтобы срок действия пароля пользователя истекал через 90 дней, выполните:

chage -M 90 <username>

Замените в этой команде <username> именем пользователя:

chage -M 90 Ivan

Чтобы периодическая смена пароля не требовалась, обычно используют значение 99999 после параметра -M.

5.3 Утилита chfn

Утилита chfn меняет информацию о пользователе: ФИО, рабочий телефон, рабочий номер комнаты, рабочий и домашний номер телефона для учетной записи пользователя. Обычный пользователь может изменить только определённые данные собственной учётной записи, разрешённые в файле /etc/login.defs (настройкой по умолчанию пользователю не разрешается менять своё имя и фамилию).

Суперпользователь может менять любые данные любой учётной записи. Кроме того, только суперпользователь может использовать параметр -o для изменения нестандартизованной части данных GECOS. Части поля GECOS не должны содержать двоеточий. За исключением части "другая", в них не должно содержаться запятых и знаков равно. Также рекомендуется избегать символов не в кодировке US-ASCII, но это касается только номеров телефонов. Часть "другая" используется для хранения информации об учётной записи, которая используется другими приложениями.

Команда chfn поддерживает следующий набор опций:

-f, --full-name – меняет ФИО пользователя.

-h, --home-phone – меняет номер домашнего телефона пользователя.

-o, --other – меняет другую информацию GECOS о пользователе. Эта часть используется для хранения информации об учётной записи, используемой другими приложениями, и может изменяться только администратором.

-r, --room – меняет номер комнаты пользователя.

-R, --root – выполнить изменения в каталоге КАТ_CHROOT и использовать файлы настройки из каталога КАТ_CHROOT.

-u, --help – показать краткую справку и закончить работу.

-w, --work-phone – меняет номер рабочего телефона пользователя.

Если ни один параметр не указан, то chfn переходит в интерактивный режим, предлагая пользователю изменить данные своей учётной записи. Вводимое значение заменяет текущее значение записи. Если введена пустая строка, то текущее значение остаётся неизменным. Текущее значение показано в скобках [ ]. При вызове без параметров программа chfn меняет учётную запись запустившего пользователя (рис. 114).

```
[root@localhost Рабочий стол]# chfn Ivan
Изменение информации finger для Ivan.
Имя [Ivan]: Anton
Office []: 1
Office Phone []: 234567
Home Phone []: 2345

Информация finger изменена.
```

Рисунок 114 – Пример изменения информации о пользователе

5.4 Утилита chsh

Команда chsh позволяет пользователям менять свои оболочки. Если оболочка не задана в командной строке, то chsh запрашивает её.

Команда chsh поддерживает следующий набор опций:

-h, --help – показать краткую справку и закончить работу;

-s, --shell – имя новой регистрационной оболочки пользователя. Если задать пустое значение, то будет использована регистрационная оболочка по умолчанию.

Если параметр **-s** не задан, то chsh переходит в интерактивный режим, предлагая пользователю изменить свою регистрационную оболочку. Вводимое значение заменяет текущее значение поля. Если введена пустая строка, то текущее значение остаётся неизменным. Текущее значение регистрационной оболочки указано в скобках [ ] (рис. 115).

```
[root@localhost Рабочий стол]# chsh
Изменение шелла для root.
Новый шелл [/bin/bash]:
```

Рисунок 115 – Выбор регистрационной оболочки

5.5 Утилита useradd

Команда useradd регистрирует нового пользователя или меняет информацию о пользователях.

Команда useradd поддерживает следующий набор опций:

-c, --comment - любая текстовая строка. Обычно, здесь коротко описывается учётная запись, и в настоящее время используется как поле для имени и фамилии пользователя.

-b, --base-dir - базовый системный каталог по умолчанию, если другой каталог не указан с помощью параметра "-d". БАЗОВЫЙ_КАТАЛОГ объединяется с именем учётной записи для определения домашнего каталога. Если не используется параметр "-m", то БАЗОВЫЙ_КАТАЛОГ должен существовать.

-d, --home - для создаваемого пользователя будет использован каталог БАЗОВЫЙ_КАТАЛОГ в качестве начального каталога. По умолчанию, это значение получается объединением ИМЕНИ пользователя с БАЗОВЫМ_КАТАЛОГОМ и используется, как имя домашнего каталога.

-e, --expiredate — дата, когда учётная запись пользователя будет заблокирована. Дата задаётся в формате ГГГГ-ММ-ДД.

-f, --inactive — число дней, которые должны пройти после окончания срока действия пароля, чтобы учётная запись заблокировалась навсегда. Если указано значение 0, то учётная запись блокируется сразу после окончания срока действия пароля, а при значении -1 данная возможность не используется. По умолчанию используется значение -1.

-G, --groups — список дополнительных групп, в которых числится пользователь. Перечисление групп осуществляется через запятую без промежуточных пробелов. На указанные группы действуют те же ограничения, что и для группы указанной в параметре -g.

-h, --help — показать краткую справку и закончить работу.

-m, --create-home — создает начальный каталог нового пользователя, если он еще не существует. Если каталог уже существует, добавляемый пользователь должен иметь права на доступ к указанному каталогу.

-K, --key — используется для изменения значений по умолчанию, хранимых в файле /etc/login.defs (UID_MIN, UID_MAX, UMASK, PASS_MAX_DAYS и других).

Пример: -K PASS_MAX_DAYS=-1 можно использовать при создании системной учётной записи, чтобы выключить ограничение на срок действия пароля, даже если системная учётная запись вообще не имеет пароля. Можно указывать параметр -K несколько раз, например: -K UID_MIN=100 -K, UID_MAX=499.

-o, --non-unique — позволяет создать учётную запись с уже имеющимся (не уникальным) UID.

-p, --password — шифрованное значение пароля, которое возвращает функция crypt. По умолчанию учётная запись заблокирована.

-s, --shell — имя регистрационной оболочки пользователя. Если задать пустое значение, то будет использована регистрационная оболочка по умолчанию.

Например, чтобы создать пользователя Ivan необходимо выполнить команду:

useradd Ivan

Для добавления пользователя в группу devel необходимо выполнить команду:

useradd -G devel Ivan

5.6 Утилита usermod

Команда usermod меняет системные файлы учётных записей согласно переданным в командной строке параметрам.

Команда usermod поддерживает следующий набор опций:

-a, --append — добавить пользователя в дополнительную группу(ы). Использовать только вместе с параметром "-G".

-c, --comment — новое значение поля GECOS.

-d, --home — новый домашний каталог учетной записи. Если указан параметр "-m", то содержимое текущего домашнего каталога будет перемещено в новый домашний каталог, который будет создан, если он ещё не существует.

-e, --expiredate — установить дату окончания действия учетной записи в EXPIRE_DATE. Дата задаётся в формате ГГГГ-ММ-ДД.

-f, --inactive — установить пароль после окончания срока действия учетной записи в INACTIVE. Если указано значение 0, то учётная запись блокируется сразу после окончания срока действия пароля, а при значении -1 данная возможность не используется. По умолчанию используется значение -1.

-g, --gid — принудительно назначит первичную группу.

-G, --groups — список дополнительных групп.

-l, --login — новое значение учетной записи.

-L, --lock — заблокировать пароль пользователя. Это делается помещением символа '!' в начало шифрованного пароля, что приводит к блокировке пароля. Не используйте этот параметр вместе с "-p" или "-U".

-o, --non-unique — при использовании с параметром "-u", этот параметр позволяет указывать не уникальный числовой идентификатор пользователя.

-p, --password — задать новый шифрованный пароль для учетной записи.

-s, --shell — задать новую оболочку для учетной записи.

-u, --uid — новый uid для учетной записи.

-U, --unlock — разблокировать учетную запись.

-Z, --selinux-user — новое Selinux-отображение учетной записи.

Например, чтобы добавить пользователя Ivan в дополнительную группу необходимо выполнить команду:

usermod -a -G ftp Ivan

5.7 Утилита userdel

Команда userdel позволяет администратору удалять существующую учетную запись пользователя. Команда userdel поддерживает следующий набор опций:

-f, --force — с этим параметром учётная запись будет удалена, даже если пользователь в этот момент работает в системе. Она также заставляет userdel удалить домашний каталог пользователя и почтовый ящик, даже если другой пользователь использует тот же домашний каталог или если почтовый ящик не принадлежит данному пользователю. Если значение USERGROUPS_ENAB равно "yes" в файле /etc/login.defs и если существует группа с именем удаляемого пользователя, то эта группа будет удалена, даже если она всё ещё является первичной группой другого пользователя. Примечание: этот параметр опасно использовать, он может привести систему в нерабочее состояние.

-h, --help - показать краткую справку и закончить работу.

-r, --remove — файлы в домашнем каталоге пользователя будут удалены вместе с самим домашним каталогом и почтовым ящиком. Пользовательские файлы, расположенные в других файловых системах, нужно искать и удалять вручную.

Команда userdel, завершая работу, возвращает следующие значения:

0 — успешное выполнение;

1 — не удалось изменить файл паролей;

2 — ошибка в параметрах команды;

6 — указанный пользователь не существует;

8 — пользователь сейчас работает в системе;

10 — не удалось изменить файл групп;

12 — не удалось удалить домашний каталог.

Например, чтобы удалить пользователя Ivan, необходимо воспользоваться командой:

userdel -r Ivan

5.8 Утилита groupadd

Команда groupadd позволяет администратору создавать новые группы в системе. Команда groupadd поддерживает следующий набор опций:

-f — вернуть статус успешного выполнения, если группа уже существует. Если используется вместе с параметром "-g" и указанный GID уже существует, то выбирается другой (уникальный) GID, то есть параметр "-g" игнорируется.

-g — числовое значение идентификатора группы. Значение должно быть уникальным, если не задан параметр "-o". Значение должно быть не отрицательным. По умолчанию берётся значение больше 999 и больше идентификатора любой другой группы. Значения от 0 и до 999 обычно зарезервированы под системные группы.

-h, --help — показать краткую справку и закончить работу.

-K — изменить значения по умолчанию (GID_MIN, GID_MAX и другие), которые хранятся в файле /etc/login.defs. Можно указать несколько параметров "-K".

Пример: -K GID_MIN=100 -K GID_MAX=499

-o — разрешить добавление группы с не уникальным GID.

5.9 Утилита groupmod

Команда groupmod позволяет администратору изменять существующие группы в системе. Команда groupmod поддерживает следующий набор опций:

-g, --gid — изменить идентификатор группы;

-h, --help — показать краткую справку и закончить работу;

-n, --new-name — изменить имя группы;

-o, --non-unique — позволяет использовать не уникальный GID;

-p, --password - шифрованное значение пароля, которое возвращает функция crypt.

Например, для изменения имени группы с testgroup на newtestgroup можно воспользоваться командой:

sudo groupmod -n newtestgroup testgroup

5.10 Утилита groupdel

Команда groupdel позволяет администратору удалить определение группы из системы путем удаления записи о соответствующей группе из файла /etc/group. Она, однако, не удаляет идентификатор группы (GID) из файла паролей. Удаленный GID действует для всех файлов и каталогов, которые его имели.

Например, удалить группу engines можно с помощью команды:

groupdel engines

5.11 Утилита chcat

Утилита chcat является программой, написанной на python. Она обеспечивает удобство добавления, удаления и просмотра категорий MLS для файлов и пользователей.

Используйте +/- для добавления/удаления категории у файла или пользователя.

При удалении категории необходимо задать '--' в командной строке до использования синтаксиса "-Category". Это сообщит команде, что вы закончили вводить опции и теперь задаете имя категории.

Утилита chcat поддерживает следующий набор опций:

-d — удалить категорию из каждого ФАЙЛА/ПОЛЬЗОВАТЕЛЯ.

-L — вывести доступные категории.

-l — сообщить команде chcat, что нужно работать с пользователями вместо файлов.

Пример просмотра доступных категорий (рис. 116).

```
[root@localhost Рабочий стол]# chcat -L
s0                          SystemLow
s0-s0:c0.c1023              SystemLow-SystemHigh
s0:c0.c1023                 SystemHigh
```

Рисунок 116 – Просмотр доступных категорий

5.12 Утилита chcon

Утилита chcon меняет SELinux контекст файла.

Команда chcon поддерживает следующий набор опций:

-h, --nodeference – использовать символические ссылки вместо указанного файла;

--reference = ФАЙЛА – использовать контекст безопасности ФАЙЛА,вместо указанного значения контекста;

-R, -recursive – рекурсивно обрабатывать файлы и каталоги;

-v, --verbose – выводить диагнотические сообщения для каждого файла;

-u, --user=ПОЛЬЗ – задать ПОЛЬЗОВАТЕЛЯ в назначаемом контексте безопасности;

-r, --role=РОЛЬ – задать РОЛЬ в назначаемом контексте безопасности;

-t, --type=ТИП – задать ТИП в назначаемом контексте безопасности;

-l, --range=ДИАПАЗОН – задать ДИАПАЗОН в назначаемом контексте безопасности;

--help – показать справку и выйти;

--version – показать информацию о версии и выйти.

Следующие ключи влияют на способ обхода иерархии каталогов при заданном ключе -R. Если указано несколько этих ключей, действует только последний.

-H – если аргумент командной строки является символьной ссылкой на каталог, перейти по ней;

-L – переходить по любой встреченной символьной ссылке на каталог;

-P – не переходить по символьным ссылкам (по умолчанию).

Например, для изменения типа файла на другой тип в назначаемом контексте безопасности (рис. 117) можно воспользоваться командой:

chcon -t samba_share_t /var/www/html/test2file

Для просмотра изменений необходимо выполнить команду:

ls -Z /var/www/html/test2file

```
[root@localhost Рабочий стол]# chcon -t samba_share_t /var/www/html/test2file
[root@localhost Рабочий стол]# ls -Z /var/www/html/test2file
-rw-r--r--. root root unconfined_u:object_r:samba_share_t:s0 /var/www/html/test2
file
```

Рисунок 117 – Изменение типа файла в назначаемом контексте безопасности

5.13 Утилита checkpolicy

Утилита checkpolicy анализирует, проверяет и компилирует политику SELinux в двоичную политику, которая может быть загружена в ядро.

Утилита checkpolicy поддерживает следующий набор опций:

-o – компиляция является опциональной;

-b – проверка двоичных политик на корректность и допустимость;

-M – проверка политики MLS;

-d – вызывается режим отладки.

Наример, для проверки двоичных политик на корректность и допустимость используется команда:

checkpolicy –b

5.14 Утилита load_policy

Утилита load_policy используется для загрузки/замены политики в ядре. По умолчанию при загрузке политики load_policy сохраняет текущие значения переключателей.

Утилита load_policy поддерживает следующий набор опций:

-b – сбросить переключатели в значения, определенные в политике;

-q – скрыть предупреждения.

Наример, для сброса переключателей в значения, определенные в политике используется команда:

load_policy –b

5.15 Утилита restorecon

Команда restorecon устанавливает контекст безопасности указанных файлов. Может также использоваться для исправления ошибок, проверки текущего содержимого файлов или добавления поддержки новой политики или с опцией "-n", чтобы убедиться в том, какой контекст присвоен файлу.

Команда restorecon поддерживает следующий набор опций:

-i – игнорировать несуществующие файлы;

-f – содержит список файлов, которые будут обработаны (для того чтобы использовать стандартный ввод, используйте - символ дефис);

-e – задать директорию, которую нужно исключить из обработки (для нескольких директорий повторите опцию);

-R, -r – рекурсивно поменять метки для файлов и директорий;

-n – не менять метки файлов;

-o – сохранить список файлов с некорректным контекстом в outfilename;

-v – показать изменения меток файлов;

-vv – показать изменения меток файлов, если изменился тип, роль или пользователь;

-F – если произошли изменения, то принудительно установить контекст как в file_context для настраиваемых файлов (customizable files) или секции пользователя.

Пример выполнения команды вывод списка файлов для обработки (рис. 118).

```
[root@localhost Рабочий стол]# restorecon -f
restorecon: option requires an argument -- 'f'
usage:  restorecon [-iFnprRv0] [-e excludedir ] [-o filename ]
[-f filename | pathname... ]
```

Рисунок 118 – Список файлов для обработки

5.16 Утилита restorecond

Утилита restorecond наблюдает за созданием новых файлов файловой системы. Наблюдение осуществляется с помощью механизма inotify. Restorecond также позволяет установить контексты недавно созданных файлов в соответствии с политикой SELinux.

Утилита restorecond поддерживает следующий набор опций:

-d – включить режим отладки. Приложение все также исполняется на переднем плане, но начинает выводиться большое число отладочных сообщений.

Пример включения режима отладки (рис. 119).

```
[root@localhost Рабочий стол]# restorecond -d
Read Config
1: Dir=/etc, File=services
2: Dir=/etc/samba, File=secrets.tdb
3: Dir=/var/run, File=utmp
4: Dir=/var/log, File=wtmp
5: Dir=/root, File=*
6: Dir=/root/.ssh, File=*
```

Рисунок 119 – Режим отладки

5.17 Утилита semodule

Утилита semodule используется для управления модулями политики SELinux. Она может использоваться для установки, обновления, перечисления или удаления модулей. Она может далее использоваться для принудительного восстановления или перезагрузки политики.

Утилита semodule поддерживает следующий набор опций:

-R, --reload – принудительно перезагрузить политику;

-B, --build – принудительно пересоздать политику (если не используется опция -n, то происходит и ее перезагрузка);

-i,--install=MODULE_PKG – установить/заменить модуль пакета;

-u,--upgrade=MODULE_PKG – обновить существующий модуль пакета;

-b,--base=MODULE_PKG – установить/заменить базовый модуль пакета;

-r,--remove=MODULE_NAME – удалить существующий модуль;

-l,--list-modules – показать список установленных модулей (кроме базовых);

-s,--store – имя хранилища, с которым производятся операции;

-n,--noreload – не перезагружать политику после выполнения операции;

-h,--help – вывести подсказку;

-v,--verbose – подробный вывод.

Пример выполнения команды: semodule -l показать список установленных модулей (рис. 120).

```
[root@localhost Рабочий стол]# semodule -l
abrt    1.2.0
accountsd       1.0.0
ada     1.4.0
afs     1.5.3
aiccu   1.0.0
aide    1.5.0
aisexec 1.0.0
amanda  1.12.0
amavis  1.10.3
amtu    1.2.0
apache  2.1.2
apcupsd 1.6.1
arpwatch        1.8.1
asterisk        1.7.1
audioentropy    1.6.0
automount       1.12.1
```

Рисунок 120 – Список установленных модулей

5.18 Утилита setenforce

Команда setenforce устанавливает режим, который выполняет политика SELinux. Режимы могут быть соблюдения и разрешения 1 (включить) или 0 (отключить) (рис. 121).

```
[root@localhost Рабочий стол]# setenforce
usage:  setenforce [ Enforcing | Permissive | 1 | 0 ]
```

Рисунок 121 – Установка режима политики SELinux

5.19 Утилита setfiles

Утилита setfiles используется для инициализации базы данных контекста безопасности для одной или более файловых систем. Она может также использоваться для проверки текущего контекста файла, исправления ошибок и добавления поддержки новой политики.

Утилита setfiles поддерживает следующий набор опций:

-c – проверить соответствие контекста тому, что определено в двоичном файле политики.

-d – показать, какая спецификация соответствует каждому файлу

-l – отразить изменения меток в syslog.

-n – не менять метки файлов.

-q – подавить вывод, не относящийся к ошибкам

-r – использовать альтернативный путь к корневой директории

-e directory – задать директорию, которую нужно исключить из обработки (для нескольких директорий повторите опцию).

-F – принудительно установить контекст как в file_context для настраиваемых файлов (customizable files).

-o filename – сохранить список файлов с некорректным контекстом в filename.

-s – получить список файлов со стандартного ввода, вместо использования пути, определяемого в командной строке.

-v – показать изменения меток файлов, если изменился тип или роль.

-vv – показать изменения меток файлов, если изменился тип, роль или пользователь.

-W – вывести предупреждения, если встретятся спецификации, которым не соответствует ни один файл.

Пример выполнения команды отображения изменения меток в syslog (рис. 122).

```
[root@localhost Рабочий стол]# setfiles -l
usage:  setfiles [-dnpqvW] [-o filename] [-r alt_root_path ]
spec_file pathname...
usage:  setfiles -c policyfile spec_file
usage:  setfiles -s [-dnpqvW] [-o filename ] spec file
```

Рисунок 122 – Отображение изменения меток в syslog

5.20 Утилита AIDE

Утилита AIDE управляет контролем целостности и используется для обнаружения злонамеренных или непреднамеренных модификаций критически важных для работы системы программ и баз данных. Подробное описание работы с утилитой AIDE рассмотрено далее в подразделе 10.3.

5.21 Утилита AMTU

Abstract Machine Test Utility (AMTU) — абстрактная машинная тестовая утилита является административной утилитой, которая проверяет, выполняются ли основополагающие защитные механизмы.

AMTU выделяет 20% свободной памяти системы, а затем записывает в неё шаблон (pattern) случайных байт. Она читает перезаписанную область памяти и проверяет соответствие считанного и записанного. Если соответствия нет, то сообщает об ошибке памяти.

Для выполнения требования разделения памяти AMTU выполняет следующее. Как обычный пользователь, AMTU выбирает случайные области памяти в диапазонах, указанных в /proc/ksyms, чтобы проверить, что программы пространства пользователя не могут читать или записывать в области памяти, используемые такими средствами, как ядро и видеопамять. Если какая-либо из вышеупомянутых попыток выполняется успешно, то сообщается об отказе.

AMTU также проверяет устройства ввода-вывода. Когда ядро обнаруживает попытку открытия сетевого соединения по заданному на локальной машине адресу, то ядро само обрабатывает пакеты вместо отправки их физическому устройству. Во избежание этой оптимизации, которая не требует удаленного сервера, она при открытии сокета определяет домен PF_PACKET.

AMTU выполняет следующее:

- при использовании домена PF_PACKET, AMTU открывает другое соединение с сервером для его прослушивания
- проверяет, что переданные случайные данные совпадают с полученными данными. Шаги 1 и 2 повторяются для каждого заданного сетевого устройства.

Для проверки дисковых контроллеров (только IDE и SCSI) AMTU открывает файл на каждой смонтированной файловой системе, доступной для чтения и записи, записывает случайную строку в 10 МБ, закрывает файл, вновь открывает файл и читает его для проверки неизменности строки.

AMTU выводит на экран предупреждение администратору, если дисковый контроллер (только для IDE) не был протестирован, из-за того что дисковый контроллер обслуживает устройства CD-ROM и дисковода.

Инструкции режима пользователя доступны только в режиме суперпользователя root. Ядро может переключиться в режим супервизора для использования специальных инструкций. Программное обеспечение пространства пользователя не имеет возможности использовать эти инструкции. Подмножество этих привилегированных инструкций должно быть протестировано для проверки их работы.

Список инструкций, которые доступны только в режиме супервизора, является архитектурно-зависимым.

Утилита AMTU поддерживает следующий набор опций:

-d Вывод сообщения об отладке;

-m Выполнение теста памяти;

-s Выполнение теста разделения памяти;

-i Запуск контроллера ввода/вывода тестирования диска;

-n Запуск контроллера ввода/вывода проверки сети;

-p Запуск в режиме суперпользователя инструкций по тестированию;

-h Вывод информации об использовании команд.

Пример выполнения команды: запуск контроллера ввода/вывода проверки сети (рис. 123).

```
[root@localhost Рабочий стол]# amtu -n
Executing Network I/O Tests...
Network I/O Controller Test SUCCESS!
```

Рисунок 123 – Запуск контроллера ввода/вывода проверки сети выполнен успешно

5.22 Утилита sudo

Утилита sudo предоставляет привилегии root для выполнения административных операций в соответствии со своими настройками. Она позволяет контролировать доступ к важным приложениям в системе.

Утилита sudo поддерживает следующий набор опций:

-V — заставляет sudo показать номер версии и выйти. Если пользователем, инициировавшим вызов, является root, то параметр "-V" отобразит список значений по умолчанию, с которыми была задана sudo, в том числе локальные сетевые адреса машины.

-l — перечислит дозволенные и запрещенные команды для пользователя на данной машине.

-L — отобразит список параметров, которые могут быть установлены в строке Defaults, с кратким описанием каждого. Этот параметр полезен в сочетании с grep(1).

-h — параметр "-h" (помощь) заставит sudo показать справку об использовании утилиты и выйти.

-v — sudo обновляет временную метку пользователя, предложив пользователю, если необходимо, указать пароль. Это продлит срок действия прежнего пароля sudo на следующие 5 минут или на тот срок, который указан в sudoers, но не требует при этом выполнения какой-либо команды.

-k — лишает законной силы временную метку пользователя, устанавливая время на начало века. При следующем выполнении sudo потребуется указать пароль. Эта операция не требует указания пароля и была добавлена, чтобы позволить пользователю аннулировать права sudo из файла .logout.

-K — полностью удаляет временную метку пользователя. Этот параметр тоже не требует указания пароля.

-b — выполнить заданную команду в фоновом режиме. Если вы используете параметр -b, то вы не сможете использовать контроль над запущенными процессами оболочки для манипуляций командами.

-p — позволяет переопределить внешний вид приглашения в систему по умолчанию. Если вид приглашения содержит управляющий символ %u, то %u будет заменен учетным именем пользователя. Аналогично %h может быть заменено на имя компьютера.

-c — заставляет sudo выполнить определенную команду с ограничением ресурсов, свойственным указанному классу пользователя. Параметр класс может быть именем класса, указанным в /etc/login.conf или знаком "-". Указание класса с помощью "-" означает, что

команда будет выполнена с учетом прав того пользователя, от имени которого эта команда выполняется. Если параметр указывает на текущий класс пользователя, то команда должна быть выполнена от имени root, или команда sudo должна выполняться из оболочки суперпользователя (root). Этот параметр доступен с BSD-классом входа в систему, где sudo был сконфигурирован с параметром "--with-logincap".

-a — принуждает sudo при идентификации пользователя использовать указанный тип аутентификации в соответствии с /etc/login.conf. Системный администратор может указать перечень подходящих для sudo методов аутентификации путём добавления в /etc/login.conf записи "auth-sudo". Этот параметр доступен только на системах поддерживающих BSD-тип аутентификации, если sudo был сконфигурирован с параметром "--with-bsdauth".

-u — вызывает sudo для выполнения указанной команды от имени пользователя, отличного от root. Для указания uid вместо имени пользователя используйте #uid.

-s — запускает командный интерпретатор, определенный переменной окружения SHELL или оболочку, указанную в passwd(5).

-H — устанавливает значение переменной окружения HOME к домашнему каталогу целевого пользователя (по умолчанию root), определенного в passwd(5). По умолчанию sudo не изменяет HOME.

-P — сообщает sudo о необходимости сохранения вектора группы пользователя в неизменном виде. По умолчанию sudo инициализирует групповой вектор к списку групп, к которым принадлежит целевой пользователь. Однако, реальный и эффективный идентификаторы групп назначаются соответствующими целевому пользователю.

-S — заставляет sudo считывать пароль со стандартного ввода вместо терминала.

В случае успешного выполнения возвращаемым значением sudo будет возвращаемое значение выполненной программы.

В противном случае sudo завершает работу со значением 1, если обнаруживает проблемы в конфигурации/правах доступа или не в состоянии выполнить заданную команду. В последнем случае сообщение об ошибке будет выведено в stderr. Если sudo не в состоянии получить stat(2) на одну или болеее запись в пользовательском PATH, то сообщение об ошибке будет выведено на stderr. Если каталог не существует или если это на самом деле не каталог, запись о нем будет игнорирована и об ошибке сообщено не будет. При нормальных обстоятельствах этого не должно произойти. Наиболее частая причина возврата от stat(2) "permission denied", если вы запустили автоматическое монтирование дисков и один из каталогов в вашем PATH находится на машине, которая в настоящий момент не доступна.

Пример выполнения команды получения списка файлов домашнего каталога пользователя Ivan с помощью параметра "-u" (рис. 124).

```
[root@localhost Рабочий стол]# sudo -u Ivan ls ~Ivan
Видео      Загрузки  Музыка         Рабочий стол
Документы  Картинки  Общедоступные  Шаблоны
```

Рисунок 124 – Список файлов домашнего каталога пользователя Ivan

5.23 Утилита getfacl

Утилита getfacl используется для просмотра установленных ACL.

Утилита getfacl поддерживает следующий набор опций:

-a, --access – вывод ACL без Default ACL.

-d, --default – вывод только Default ACL.

--omit-header – не выводить заголовок с комментариями (первые три строки вывода).

--all-effective – выводить комментарии с действующими правами доступа для каждого пользователя, даже если они совпадают с заданными.

--no-effective – не выводить комментарии с действующими правами доступа ни для одного пользователя.

--skip-base – не выводить данные файлов, у которых установлены только основные права доступа (ACL_USER, ACL_GROUP и ACL_OTHER).

-R, --recursive – делать рекурсивный обход каталога и выводить ACL для каждого файла и каталога. Можно использовать для создания резервной копии ACL всех файлов каталога.

--post-order – делать рекурсивный обход каталога и выводить ACL для каждого файла и каталога в обратном порядке, т.е. сначала выводятся ACL для файлов в каталоге, а потом для самого каталога.

-L, --logical – двигаться по символьным ссылкам на каталоги. При отсутствии данной опции выводятся только ACL каталога, на который указывает ссылка, и обход внутрь не делается.

-P, --phisycal – не двигаться по символьным ссылкам и не показывать ACL каталогов или файлов, на которые указывает ссылка.

--tabular – вывод в альтернативном табличном формате. Первый столбец - название элемента ACL, второй - имя пользователя или группы, третий - режим доступа, четвертый - Default ACL.

Пример использования команды вывода комментарий с действующими правами доступа к файлу для пользователя (рис. 125).

```
[root@localhost Рабочий стол]# getfacl --all-effective /etc/fstab
getfacl: Removing leading '/' from absolute path names
# file: etc/fstab
# owner: root
# group: root
user::rw-
group::r--
other::r--
```

Рисунок 125 – Права пользователя по отношению к файлу fstab

5.24 Утилита setfacl

Утилита setfacl предназначена для установки, модификации или удаления ACL.

Утилита setfacl поддерживает следующий набор опций:

-m – модифицировать правило acl;

-M – просмотр acl записи для редактирования из файла;

-b – удаляет все acl правила;

-k – удаляет правила "по умолчанию";

-s – заменяет правила acl заданными;

-d – устанавливает правила по умолчанию;

-R – выполняет применение acl рекурсивно;

-x – удаляет указанное acl правило;

-X – просмотр acl записи для удаления из файла;

-n – отсутствие маски для эффективных прав;

-L – логический переход по символьным ссылкам;

-P – физический переход не по символьным ссылкам;

-v – вывод версии и выход;

-h, --help – вывод справки об использовании утилиты и выход.

Примером является назначение пользователю Ivan права на чтение и запись с помощью команды setfacl -m u:Ivan:rw myfile.odt.

5.25 Утилита hwclock

Команда hwclock для обычного пользователя выводит на экран текущее аппаратное время. Пользователю с правами администратора hwclock позволяет установить текущее аппаратное время. Она также позволяет администратору установить системное время на основе аппаратного.

Команда hwclock поддерживает следующий набор опций:

--help – вывести подсказку по утилите;

--hctosys – установить системное время в соответствии с аппаратными часами;

--systohc, --debug – установить аппаратные часы в соответствии с системным временем с выводом отладочной информации;

--set --date="2011-01-25 08:55:01" – установка конкретного значения аппаратного времени;

--set --date="$(date --utc +'%F %T')" – установка конкретного значения аппаратного времени.

Пример установки времени (рис. 126).

```
[root@localhost Рабочий стол]# date 020713452014
Птн Фев  7 13:45:00 MSK 2014
[root@localhost Рабочий стол]# hwclock --localtime --systohc
```

Рисунок 126 – Установка времени

5.26 Утилита rnano

Редактор rnano является системным редактором. Он предлагает полноэкранные возможности редактирования. Однако его функции ограничены: он не будет сохранять в файлы, кроме определенных в качестве параметров командной строки, не будет обрабатывать файлы nanorc, не позволяет приостанавливать свою работу, не разрешает добавлять в файлы или сохранять от другого имени, не поддерживает резервное копирование файлов, а также проверку правописания.

Редактор rnano поддерживает следующий набор опций:

-h, -?, --help – показывать это сообщение;

+СТРОКА,СТОЛБЕЦ – начать с указаной строки и ряда;

-A, --smarthome – включить умную кнопку home;

-B, --backup – сохранять резервные копии существующих файлов;

-C <дир>, --backupdir=<дир> – каталог для хранения уникальных резервных копий;

-D, --boldtext – использовать жирный шрифт вместо обычного;

-E, --tabstospaces– преобразовать табуляции в пробелы;

-F, --multibuffer– разрешить несколько файловых буферов;

-H, --historylog– сохранять и читать историю поиска/замены строк;

-I, --ignorercfiles – не использовать файлы nanorc;

-K, --rebindkeypad– исправлять проблему малой клавиатуры;

-L, --nonewlines– не добавлять пустые строки в конце файла;

-N, --noconvert– не преобразовывать из DOS/Mac формата;

-O, --morespace– использование дополнительной строки для редактирования;

-Q <стр>, --quotestr=<стр>– строка цитирования;

-R, --restricted– ограниченный режим;

-S, --smooth– построчная прокрутка вместо полу-экранной;

-T <#чис>, --tabsize=<#чис>– установить ширину табуляции в #число столбцов;

-U, --quickblank– использовать быструю очистку строки состояния;

-V, --version– показать версию и выйти;

-W, --wordbounds– использовать более точное определение границ слов;

-Y <стр>, --syntax=<стр>– использовать описание синтаксиса для подсветки;

-c, --const– постоянно показывать позицию курсора;

-d, --rebinddelete– исправить проблему Backspace/Delete;

-i, --autoindent– автоматический отступ на новых строках;

-k, --cut– вырезать от курсора до конца строки;

-l, --nofollow– не следовать по символьным ссылкам, переписывать;

-m, --mouse– разрешить использование мыши;

-o <дир>, --operatingdir=<дир> – установить рабочий каталог;

-p, --preserve – зарезервировать кнопки XON (^Q) и XOFF (^S);

-q, --quiet– игнорировать ошибки запуска, например, rc-файла;

-r <#столбцы>, --fill=<#столбцы>– установить точку переноса строки на #столбцы;

-s <программа>, --speller=<программа>– использовать альтернативную программу проверки орфографии;

-t, --tempfile– автозапись при выходе;

-u, --undo – разрешить функцию отмены действий [ЭКСПЕРИМЕНТАЛЬНАЯ];

-v, --view– режим просмотра (только чтение);

-w, --nowrap– не переносить длинные строки;

-x, --nohelp– не показывать две строки помощи внизу;

-z, --suspend – разрешить приостановку;

-$, --softwrap – включить мягкий перенос строк;

-a, -b, -e,-f, -g, -j, (игнорируется для совместимости с Pico).

Пример работы с редактором Rnano. Создание текстового файла с названием testfile. Необхожимо ввести в консоли команду:

rnano

Откроется пустой экран, в котором можно начать печатать. Введите свой текст и по окончанию выберите ^O (клавиша Ctrl + O). Текст "считывается" в буфер (рис. 127).

Рисунок 127 – Запись текста в окно редактора Rnano

Информация в буфере изменилась. Чтобы созхранить изменения в текстовый файл, необходимо выбрать Y (клавиша Ctrl + Y). Внизу появится надпись с запросом на название файла (рис. 128).

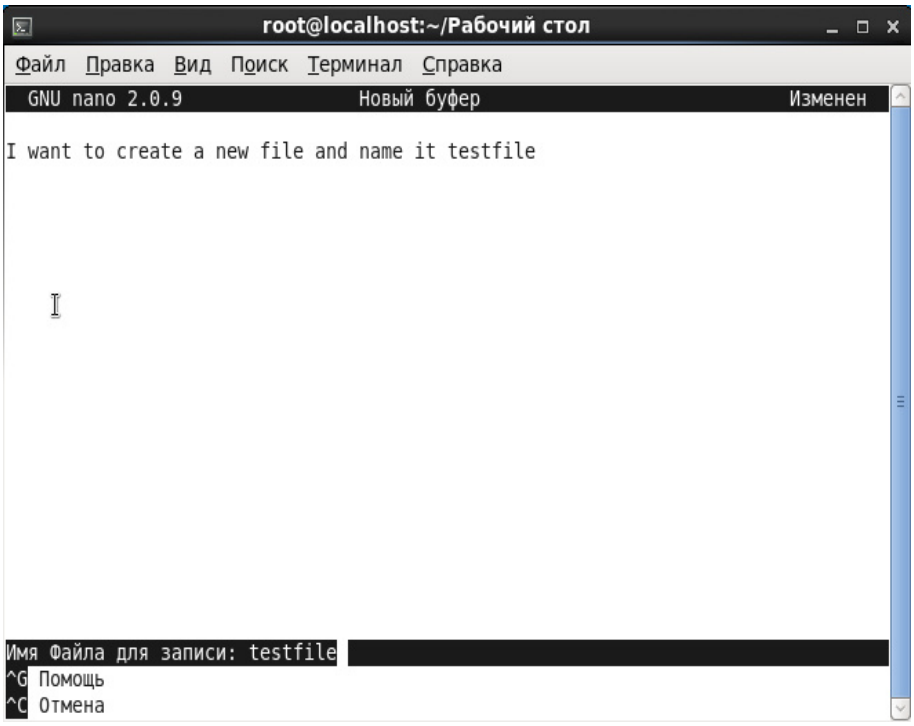


Рисунок 128 – Название созданного файла

Для открытия только что сохраненного файла, необходимо ввести в консоли:

rnano testfile

5.27 Приложение «Администрирование SELinux»

Для настройки управления безопасностью доступа к объектам системы на основе ролей предназначено приложение «Администрирование SELinux», которое запускается из меню «Система–>Администрирование–>Управление SELinux» и доступно только в режиме администратора.

Окно настройки ролей SELinux пользователей приведено на рис. 131.

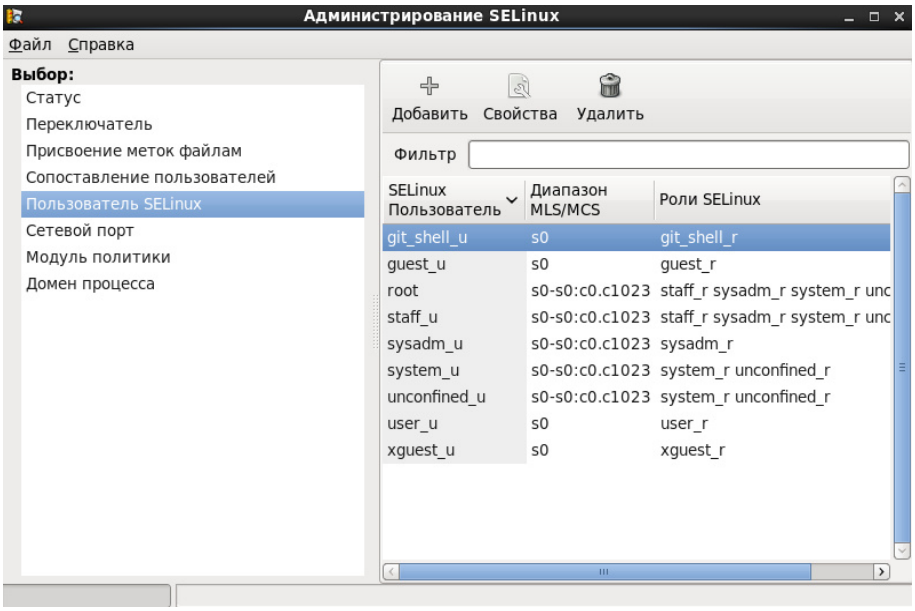


Рисунок 129 – Окно приложения "Администрирование SELinux"

Подробное описание работы приложения приведено в подразделе 4.6.

5.28 Конфигурационный файл /etc/sudoers

Настройка привилегий пользователей и наделение их полномочиями, осуществляется в конфигурационном файле /etc/sudoers (рис. 130).

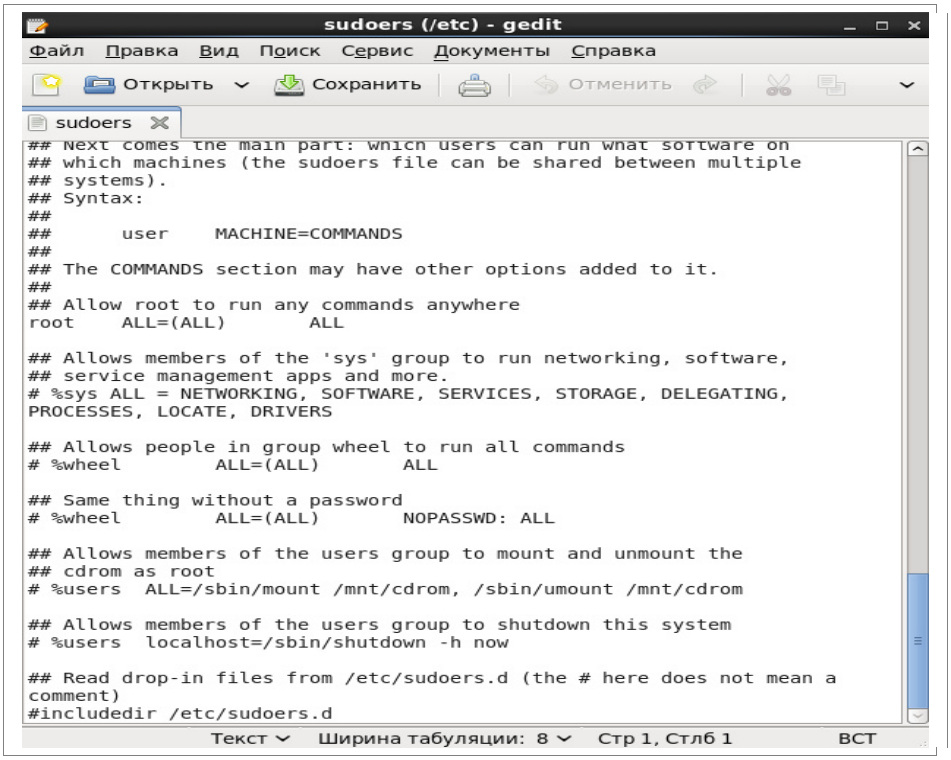


Рисунок 130 – Конфигурационный файл /etc/sudoers

Редактирование файла /etc/sudoers.

Простейшая конфигурация выглядит так:

Defaults env_reset

User privilege specification

root ALL=(ALL) ALL

user ALL=(ALL) ALL

Такая конфигурация дает пользователю user все права пользователя root при выполнении команды sudo. Defaults env_reset полностью запрещает все пользовательские переменные при исполнении команд от имени root. Это хорошо с точки зрения безопасности, однако, иногда вызывает проблемы. Можно разрешить использование личных переменных какой-либо группе или отдельному пользователю, добавив строку:

Defaults:%admin !env_reset

которая будет сохранять переменные окружения для всех пользователей группы admin, или:

Defaults:user env_keep=TZ

которая сохранит переменную TZ для пользователя user.

Если сервер администрируется группой людей, то имеет смысл поступить таким образом:

%admin ALL=(ALL) ALL

Эта запись дает доступ к root-привилегиям всем членам группы admin.

Можно настроить для каждого конкретного пользователя доступ только к конкретным командам. Например:

user ALL = /bin/mount, /bin/kill

даст пользователю user права на выполнение команд mount и kill с любой машины, а:

user2 mydebiancomp = /sbin/modprobe

даст пользователю user2 права на выполнение modprobe с машины mydebiancomp.

Синтаксис:

пользователь хост = команда

где команда прописывается с полным путем. Для группы действия аналогичны, только добавляется знак "%".

5.29 Приложение «Менеджер пользователей»

Настройка атрибутов безопасности пользователей и управление группами пользователей может осуществляться в приложении "Менеджер пользователей", которое запускается из меню «Система–>Администрирование–>Пользователи и группы» и доступно только в режиме администратора. Параметры настройки показаны на рис. 131, 132.

Подробное описание настройки представлено в подразделе 3.4.

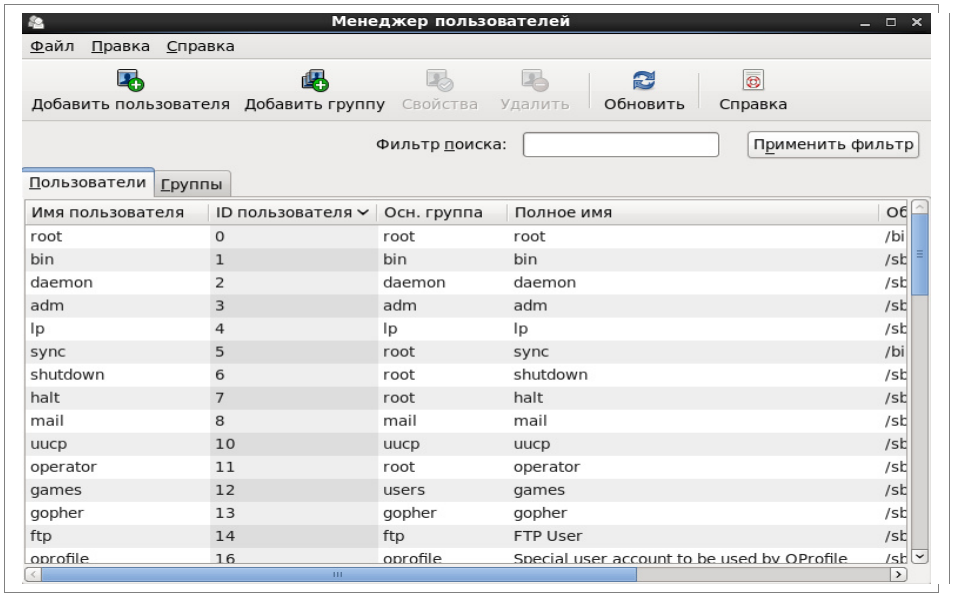


Рисунок 131 – Вкладка пользователи менеджера пользователей

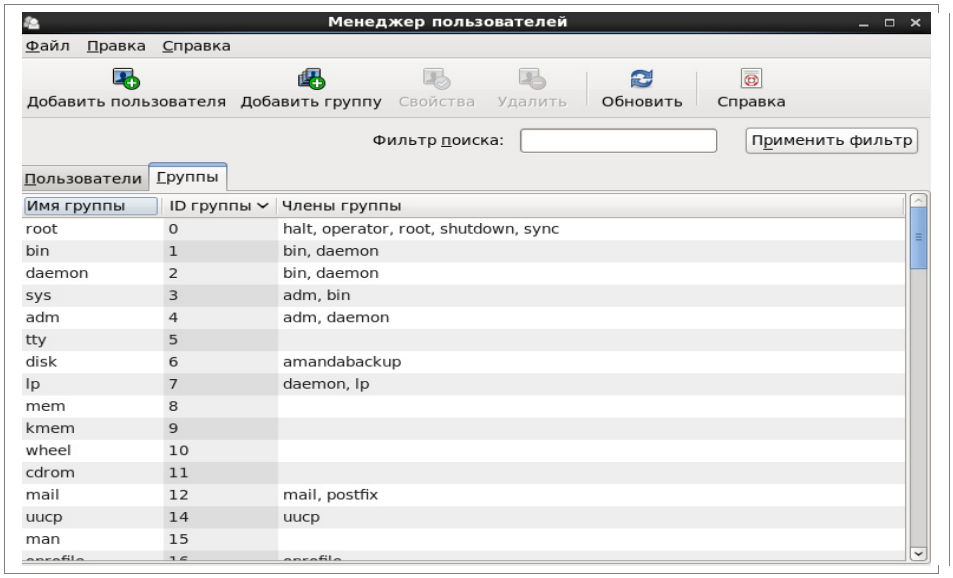


Рисунок 132 – Вкладка группы менеджера пользователей

5.30 Средства управления аудитом

Для настройки определения и обновления средств управления аудитом системы (выбор событий аудита, управление журналами аудита, анализ журнала аудита и генерация отчетов аудита) используются файлы /etc/audit/audit.rules и /etc/audit/auditd.conf (рис. 133 и 134).

Подробное описание настройки представлено далее в подразделе 6.2.

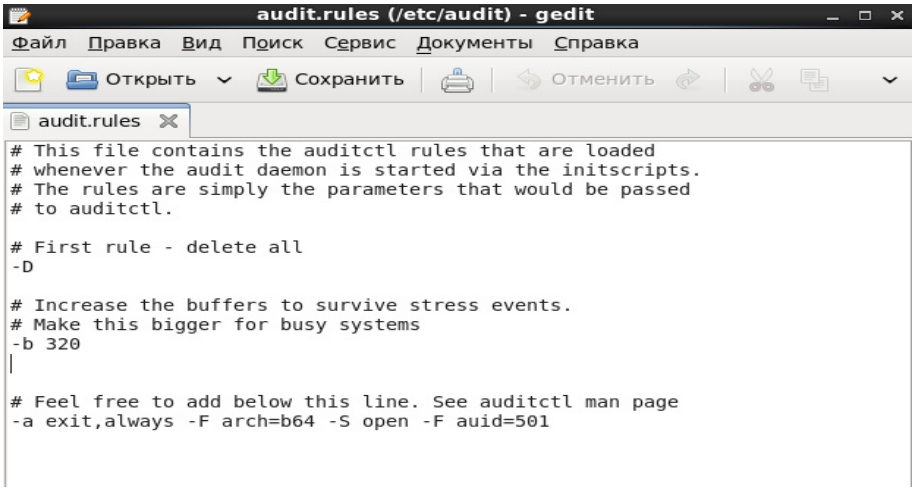


Рисунок 133 – Файл /etc/audit/audit.rules

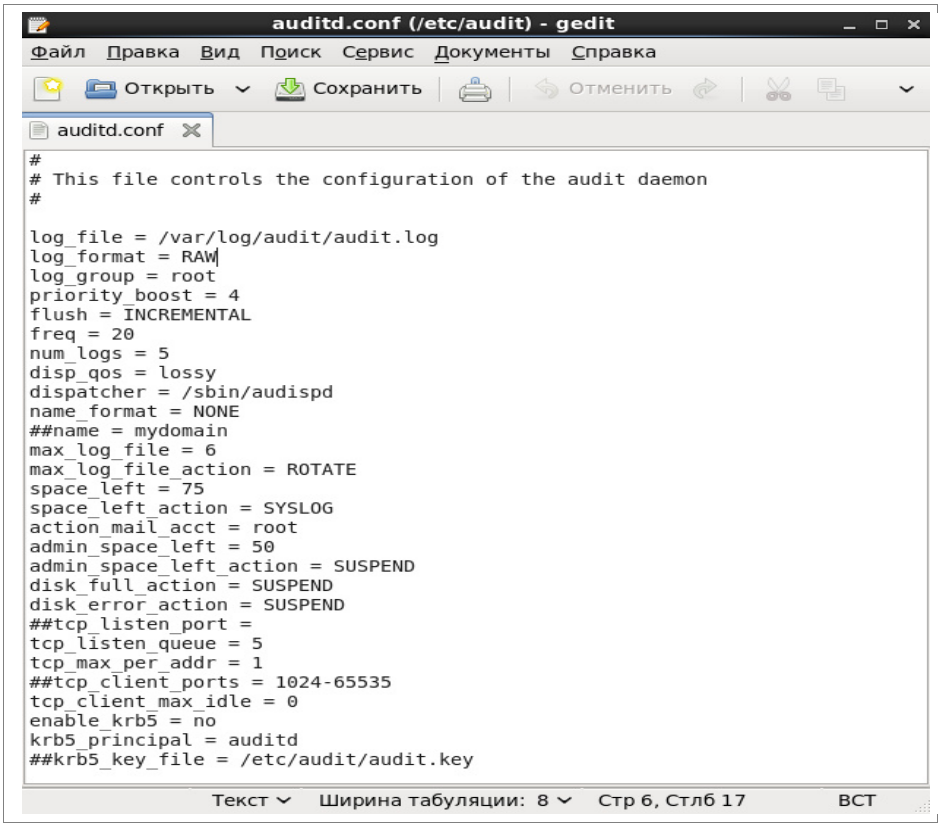


Рисунок 134 – Файл /etc/audit/auditd.conf

5.31 Приложение «Дата и время»

Окно настройки аппаратных часов позволяет установить время, дату, часовой пояс (Система->Администрирование->Дата и время), как на рис. 135 и 136.

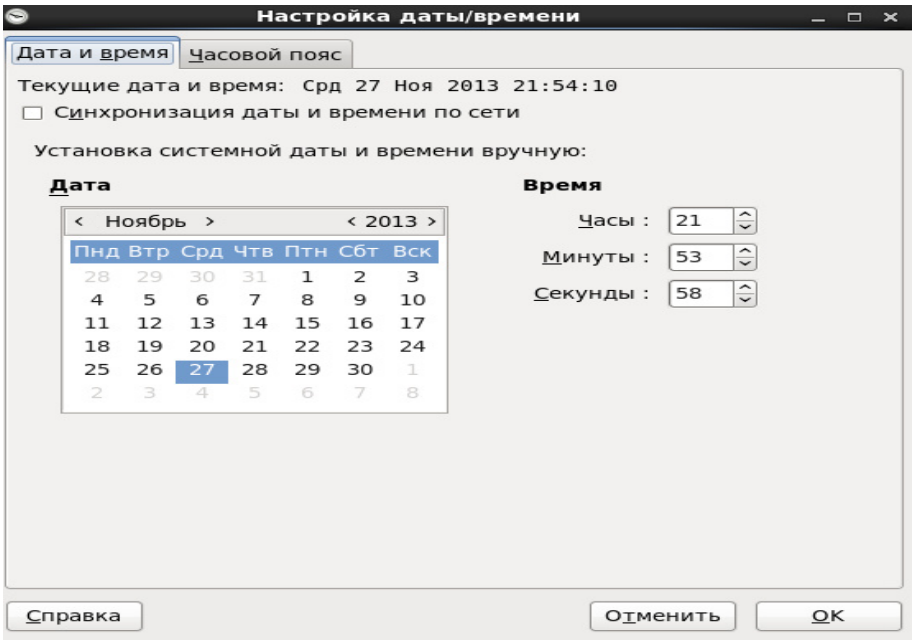


Рисунок 135 – Настройка даты/времени

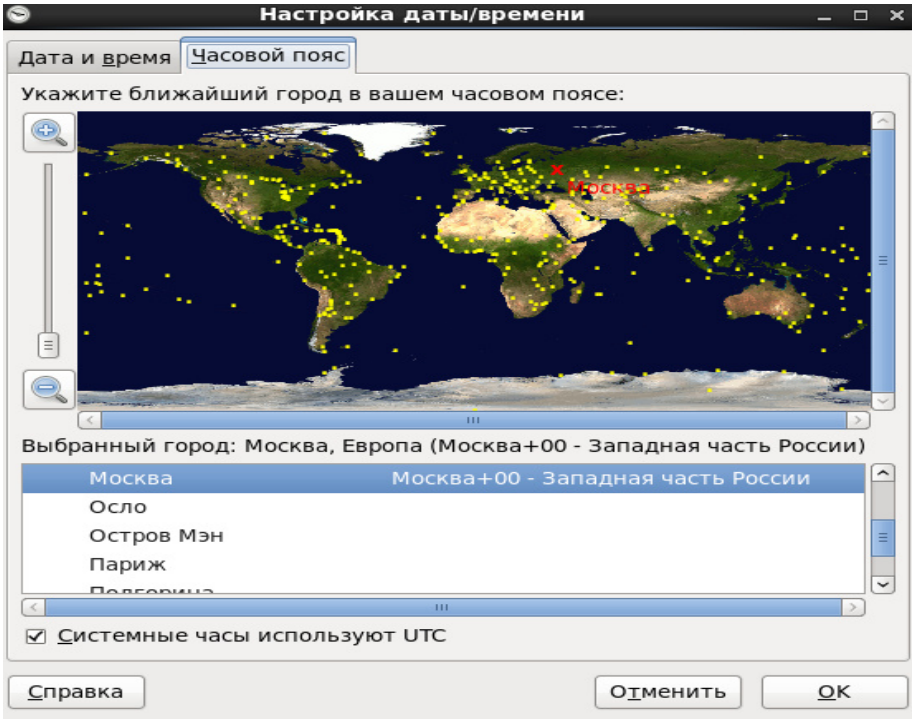


Рисунок 136 – Выбор часового пояса

Изм.	Лист	№ докум	Подп	Дата

6 АУДИТ БЕЗОПАСНОСТИ

6.1 Основные сведения

Средства аудита безопасности МСВСфера 6.3 АРМ предоставляют следующие возможности:

- определение событий безопасности, подлежащих регистрации;
- определение состава и содержания информации о событиях безопасности, подлежащих регистрации;
- сбор, запись и хранение информации о событиях безопасности;
- реагирование на сбои при регистрации событий безопасности;
- мониторинг (просмотр, анализ) результатов регистрации событий безопасности;
- защита информации о событиях безопасности;
- обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей.

Вышеперечисленные возможности аудита безопасности реализуются с помощью следующих программных компонент:

- конфигурационные файлы;
- утилита aureport;
- утилита auserch;
- утилита autrase;
- утилита auditctl;
- приложение «Администрирование Selinux»;
- приложение «Audit logs»;
- приложение «KSystemLog».

6.2 Конфигурационные файлы

Подсистема аудита включает несколько конфигурационных файлов:

/etc/sysconfig/auditd — содержит настройки, используемые при старте демона auditd;

/etc/audit/auditd.conf — настройки поведения демона auditd;

/etc/audit/audit.rules — файл, содержащий правила аудита.

Для настройки аудита необходимо настроить демон аудита auditd, т.е изменить параметры в файлах конфигурации /etc/sysconfig/auditd и /etc/audit/auditd.conf.

Файл /etc/sysconfig/auditd с содержимым по умолчанию изменять не рекомендуется (рис. 137).

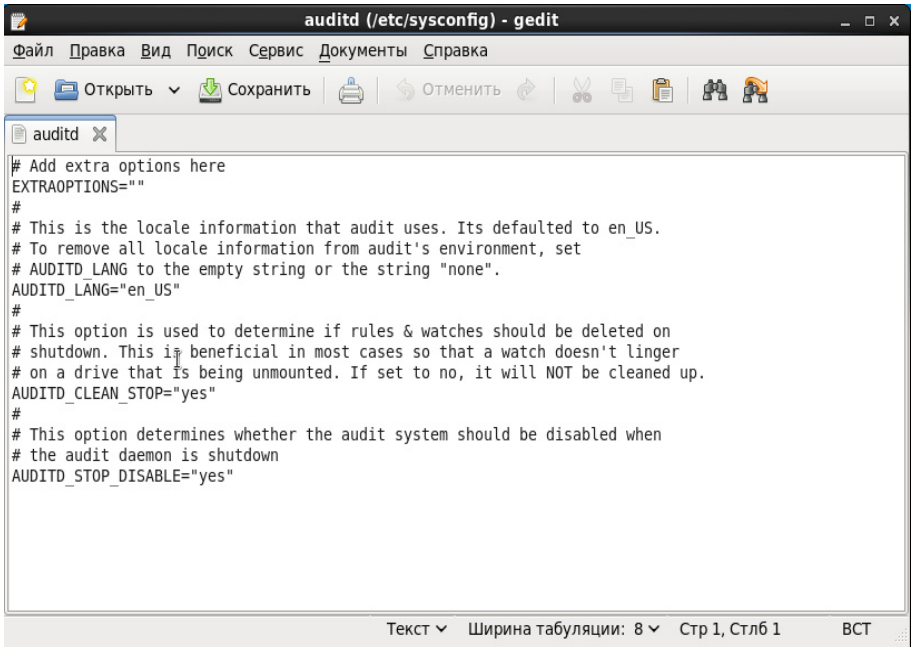


Рисунок 137 - Содержимое файла /etc/sysconfig/auditd

Перейдем ко второму файлу - /etc/audit/auditd.conf (рис. 138).

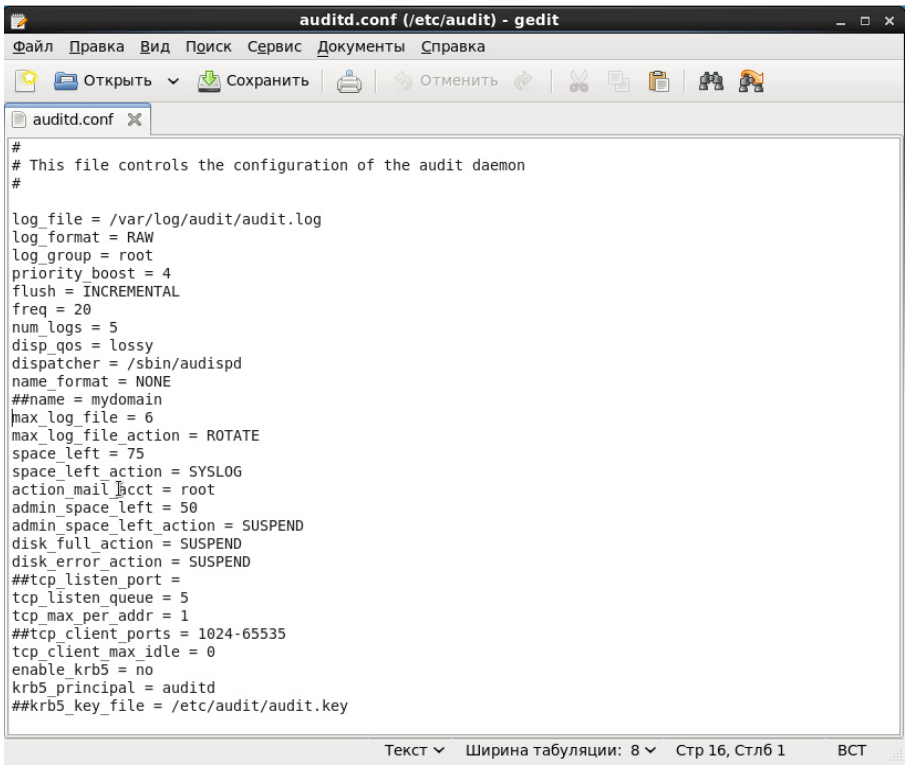


Рисунок 138– Содержимое файла /etc/audit/auditd.conf

Значения параметров, которые можно при необходимости изменить:

log_file — место расположения и название файла аудита (лог-файла, лога);

log_format — формат ведения лога. Возможные значения: RAW — сообщения записываются в том виде как их передало ядро; nolog — не писать сообщения;

log_group — группа-владелец лог-файла аудита;

priority_boost — приоритет, с каким работает демон (nice).

flush — как будет записываться лог-файл на диск. Возможные значения: none — не использовать политики записи, incremental — лог будет записываться с определенной периодичностью, определенной в параметре freq; data — данные пишутся в файл в синхронном режиме; sync — в синхронном режиме находятся не только данные, но и метаданные файла.

freq — число событий, при котором осуществляется запись данных на диск, используется при значении flush = incremental.

num_logs — число лог-файлов аудита, хранимых на диске, если настроена ротация в параметре max_log_file_action.

disp_qos — определяет надежность передачи данных между даемоном auditd и диспетчером audispd. Возможные значения: lossy — auditd может не передавать некоторые события аудита, если очередь событий полна, при этом события будут записаны на диск; lossless — логирование событий на диск будет остановлено, пока не освободится место в очереди.

dispatcher — где располагается исполняемый файл диспетчера.

name_format и name. name_format — определяет порядок разрешения имен хостов. Возможные значения: none — имя не используется; hostname — имя, возвращенное через запрос gethostname; fqd — полное имя хоста, возвращенное через DNS запрос; numeric — ip адрес; user — строка, определенная в параметре name.

max_log_file и max_log_file_action. max_log_file — максимальный размер лог-файла в мегабайтах, по достижению которого будет выполнено действие, определенное в max_log_file_action. Возможные действия: ignore — ничего не делать; syslog — отправить предупреждение в syslog; suspend — остановить запись событий на диск; rotate — произвести ротацию лог-файлов в соответствии с числом num_logs; keep_logs — осуществить ротацию, при этом не удалять старые файлы.

space_left, space_left_action и action_mail_acct. space_left — величина в мегабайтах, определяющая размер оставшегося дискового пространства, при достижении которого будет выполнно действие space_left_action. Возможные действия: ignore — ничего не делать; syslog

— отправить предупреждение в syslog; email — отправить письмо аккаунту, определенному в action_mail_acct; exec — выполнить скрипт; suspend — остановить запись на диск, перевести систему в single mode; halt — выключить систему.

admin_space_left и admin_space_left_action. admin_space_left — величина в мегабайтах оставшегося свободного пространства на диске. Предупреждение для администратора, что надо добавить/очистить свободное пространство. Величина должна быть меньше, чем space_left. Действия, которые можно определить в admin_space_left_action, аналогичны space_left_action.

disk_full_action — действия, выполняемые при заполнении всего дискового пространства, аналогичны space_left_action.

disk_error_action — действия, выполняемые при возникновении дисковой ошибки, аналогичны space_left_action.

tcp_listen_port, tcp_listen_queue, tcp_max_per_addr, tcp_client_ports и tcp_client_max_idle — демон аудита может принимать сообщения от других демонов. Данные переменные определяют сетевые настройки.

enable_krb5, krb5_principal, krb5_key_file — переменные, определяющие аутентификацию по протоколу kerberos.

6.3 Утилита aureport

Для генерации отчетов по журналу аудита в состав МСВСфера 6.3 АРМ включена утилита aureport. Для запуска данной программы необходимо зайти в программу «Терминал среды Gnome» с правами администратора и в ней выполнить команду aureport с набором опций. Команда aureport поддерживает следующий набор опций:

- -au, --auth. Отчет о всех попытках аутентификации
- -a, --avc. Отчет о всех avc сообщениях
- -c, --config. Отчет об изменениях конфигурации
- -cr, --crypto. Отчет о событиях, связанных с шифрованием
- -e, --event. Отчет о событиях
- -f, --file. Отчет о файлах
- --failed. Для обработки в отчетах выбирать только неудачные события. По умолчанию показываются и удачные, и неудачные события
- -h, --host. Отчет о хостах
- -i, --interpret. Транслировать числовые значения в текстовые

- -if, --input файл. Использовать указанный файл вместо логов аудита. Это может быть полезно при анализе логов с другой машины или при анализе частично сохраненных логов
- -l, --login. Отчет о попытках входа в систему
- -m, --mods. Отчет об изменениях пользовательских учетных записей.
- -ma, --mac. Отчет о событиях в системе, обеспечивающей МАС
- -p, --pid. Отчет о процессах
- -r, --response. Отчет о реакциях на аномальные события
- -s, --syscall. Отчеты о системных вызовах
- --success. Для обработки в отчетах выбирать только удачные события. По умолчанию показываются и удачные, и неудачные события
- --summary. Генерировать итоговый отчет, который дает информацию только о количестве элементов в том или ином отчете
- -t, --log. Этот параметр генерирует отчет о временных рамках каждого отчета.
- -te, --end [дата] [время]. Искать события, которые произошли раньше или во время указанной временной точки
- -tm, --terminal. Отчет о терминалах
- -ts, --start [дата] [время]. Искать события, которые произошли после или во время указанной временной точки
- -u, --user. Отчет о пользователях
- -v, --version. Вывести версию программы и выйти
- -x, --executable. Отчет об исполняемых объектах.

Пример выполнения команды "aureport" без параметров (вывод на экран суммарного отчета) (рис. 139).

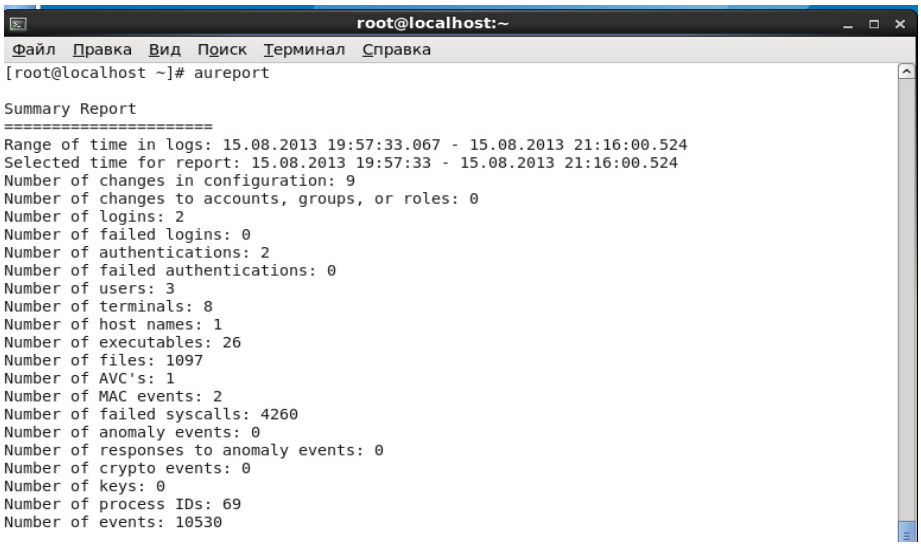


Рисунок 139 – Суммарный отчет

Пример выполнения команды aureport -au вывод отчета о всех попытках аутентификации (рис. 140).

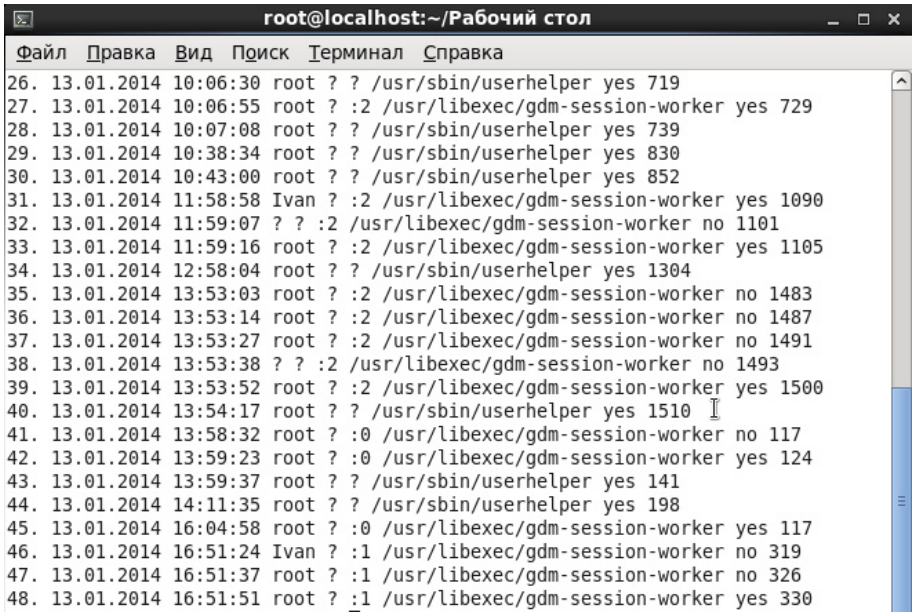


Рисунок 140 – Отчет о всех попытках аутентификации

6.4 Утилита auserch

Утилита ausearch используется для поиска по различным критериям записей в журнале аудита. Для запуска необходимо запустить в режиме root программу «Терминал среды Gnome» и в ней выполнить команду ausearch с набором опций. Команда ausearch поддерживает следующий набор опций:

- -a, --event audit-event-id. Искать события с заданным идентификатором события. Сообщения обычно начинаются примерно так:
  msg=audit(1116360555.329:2401771). Идентификатор события - это число после ':'. Все события аудита, связанные с одним системным вызовом, имеют одинаковый идентификатор;
- -c, --comm comm-name. Искать события с заданным comm name (именем) исполняемого файла задачи;
- -f, --file file-name. Искать события с заданным именем файла;
- -ga, --gid-all all-group-id. Искать события с заданным эффективным или обычным идентификатором группы;
- -ge, --gid-effective effective-group-id. Искать события с заданным эффективным идентификатором группы или именем группы;
- -gi, --gid group-id. Искать события с заданным идентификатором группы или именем группы;
- -h, --help. Справка;
- -hn, --host host-name. Искать события с заданным именем узла. Имя узла может быть именем узла, полным доменным именем или цифровым сетевым адресом;
- -i, --interpret. Транслировать числовые значения в текстовые. Например, идентификатор пользователя будет оттранслирован в имя пользователя. Трансляция выполняется с использованием данных с той машины, где запущен ausearch. Т.е. если вы переименовали учетные записи пользователей или не имеете таких же учетных записей на вашей машине, то вы можете получить результаты, вводящие в заблуждение;
- -if, --input file-name. Использовать указанный файл вместо логов аудита. Это может быть полезно при анализе логов с другой машины или при анализе частично сохраненных логов;
- -k, --key key-string. Искать события с заданным ключевым словом;

- -m, --message message-type | comma-sep-message-type-list. Искать события с заданным типом. Вы можете указать список значений, разделенных запятыми. Можно указать несуществующий в событиях тип ALL, который позволяет получить все сообщения системы аудита. Список допустимых типов большой и будет показан, если указать эту опцию без значения. Тип сообщения может быть строкой или числом;
- -o, --object SE-Linux-context-string. Искать события с заданным контекстом (объектом);
- -p, --pid process-id. Искать события с заданным идентификатором процесса;
- -pp, --ppid parent-process-id. Искать события с заданным идентификатором родительского процесса;
- -r, --raw. Необработанный вывод. Используется для извлечения записей для дальнейшего анализа;
- -sc, --success syscall-name-or-value. Искать события с заданным системным вызовом. Вы можете указать его номер или имя. Если вы указали имя, оно будет проверено на машине, где запущен ausearch;
- -se, --context SE-Linux-context-string. Искать события с заданным контекстом SELinux (stcontext/subject или tcontext/object);
- -su, --subject SE-Linux-context-string. Искать события с заданным контекстом SELinux - scontext (subject);
- -sv, --success success-value. Искать события с заданным флагом успешного выполнения. Допустимые значения: yes (успешно) и no(неудачно);
- -te, --end [end-date] [end-time]. Искать события, которые произошли раньше или во время указанной временной точки;
- -ts, --start [start-date] [start-time]. Искать события, которые произошли после или во время указанной временной точки;
- -tm, --terminal terminal. Искать события с заданным терминалом. Некоторые демоны (такие как cron и atd) используют имя демона как имя терминала;
- -ua, --uid-all all-user-id. Искать события, у которых любой из идентификаторов пользователя, эффективного идентификатора пользователя или loginuid (auid) совпадают с заданным идентификатором пользователя;
- -ue, --uid-effective effective-user-id. Искать события с заданным эффективным идентификатором пользователя;
- -ui, --uid user-id. Искать события с заданным идентификатором пользователя;

- -ul, --loginuid login-id. Искать события с заданным идентификатором пользователя. Все программы, которые его используют, должны использовать pam_loginuid;
- -v, --verbose. Показать версию и выйти;
- -w, --word. Совпадение с полным словом. Поддерживается для имени файла, имени узла, терминала и контекста SELinux;
- -x, --executable executable. Искать события с заданным именем исполняемой программы.

Пример выполнения команды ausearch с ключом "-m ALL" (вывод на экран всех событий из журнала аудита) на рис. 141.

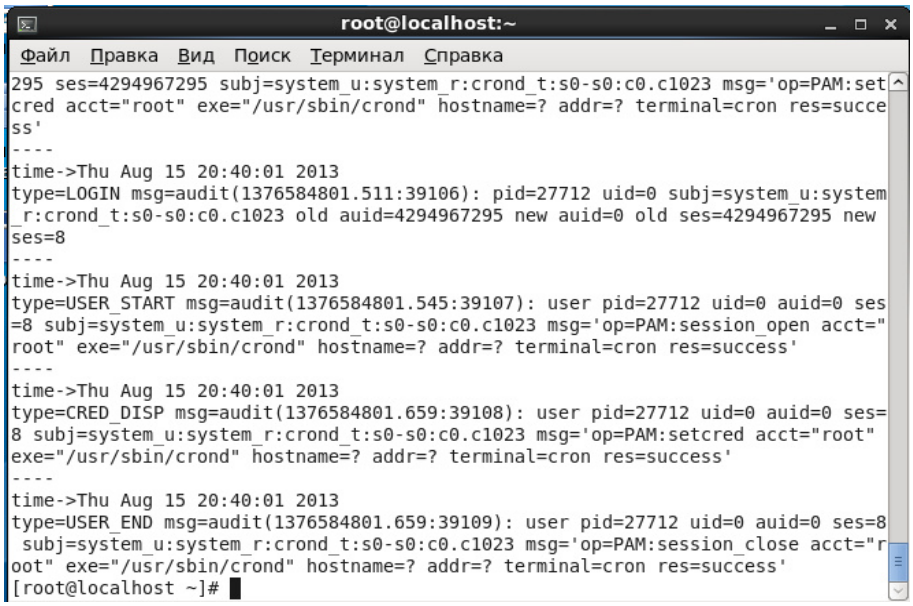


Рисунок 141 – События журнала аудита

Пример выполнения команды ausearch с ключом "-p 2653" (вывод на экран всех событий из журнала аудита, которые были сгенерированы для процесса с идентификатором 2653) представлен на рис. 142.

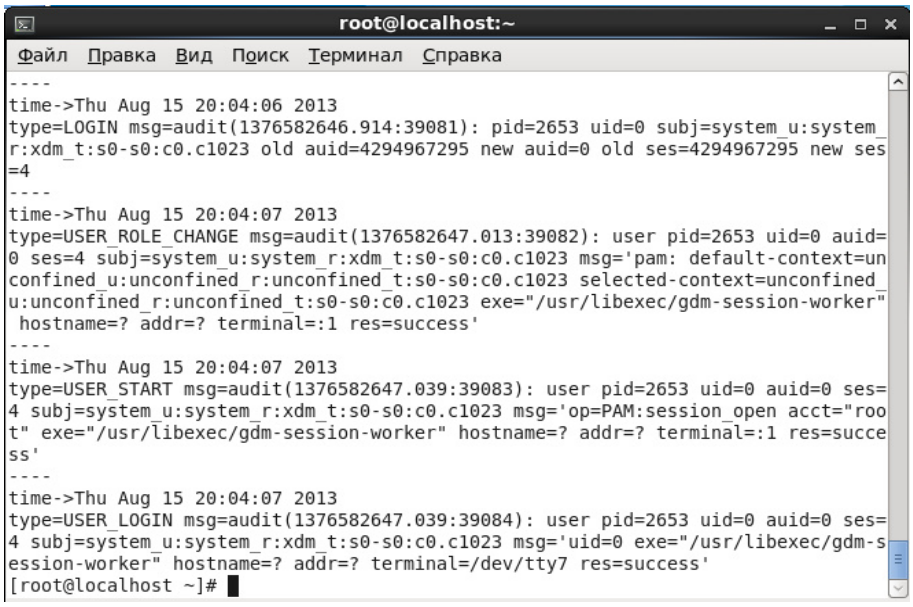


Рисунок 142 – События журнала аудита

6.5 Утилита autrace

Утилита autrace добавляет правила аудита для того, чтобы следить за использованием системных вызовов в указанном процессе. После добавления правил запускает процесс с указанными аргументами. Результаты аудита будут либо в логах аудита, если демон аудита запущен, либо в системных логах. Внутри autrace устроена так, что удаляет все предыдущие правила аудита, перед тем как запустить указанный процесс и после его завершения. Поэтому в качестве дополнительной меры предосторожности программа не запустится, если перед ее использованием правила не будут удалены с помощью audtictl - предупреждающее сообщение известит об этом.

Для запуска данной программы необходимо запустить в режиме root программу «Терминал среды Gnome» и в ней выполнить команду autrace. Autrace поддерживает опцию:

-r - ограничить сбор информации о системных вызовах только теми, которые необходимы для анализа использования ресурсов. Это может быть полезно при моделировании внештатных ситуаций, к тому же позволяет уменьшить нагрузку на логи.

Пример обычного использования:

autrace /bin/ls /tmp

ausearch --start recent -p 2442 -i

Пример для режима ограниченного сбора информации:

autrace -r /bin/ls

ausearch --start recent -p 2450 --raw | aureport --file --summary

ausearch --start recent -p 2450 --raw | aureport --host --summary

6.6 Утилита auditctl

Утилита auditctl позволяет узнать текущее состояние аудита, добавить или удалить правила фиксации событий аудита. Для запуска данной утилиты необходимо запустить в режиме root программу «Терминал среды Gnome» и в ней выполнить команду auditctl. Auditctl поддерживает следующий набор опций:

- -b backlog. Установить максимальное количество доступных для аудита буферов, ожидающих обработки (значение в ядре по умолчанию - 64). Если все буфера заняты, то флаг сбоя будет выставлен ядром для его дальнейшей обработки;
- -e [0..2]. Установить флаг блокировки. 0 позволит на время отключить аудит, включить его обратно можно, передав 1 как параметр. Если установлено значение опции 2, то защитить конфигурацию аудита от изменений. Каждый, кто захочет воспользоваться этой возможностью, может поставить эту команду последней в audit.rules. После этой команды все попытки изменить конфигурацию будут отвергнуты с уведомлением в журналах аудита. В этом случае, чтобы задействовать новую конфигурацию аудита, необходимо перезагрузить систему аудита;
- -f [0..2]. Установить способ обработки для флага сбоя. 0=silent 1=printk 2=panic. Эта опция позволяет определить, каким образом ядро будет обрабатывать критические ошибки. Например, флаг сбоя выставляется при следующих условиях: ошибки передачи в пространство демона аудита, превышение лимита буферов, ожидающих обработки, выход за пределы памяти ядра, превышение лимита скорости выдачи сообщений. Значение по умолчанию: 1. Для систем с повышенными требованиями к безопасности, значение 2 может быть более предпочтительным;
- -h. Краткая помощь по аргументам командной строки;
- -i. Игнорировать ошибки при чтении правил из файла;
- -l. Вывести список всех правил по одному правилу в строке;
- -k ключ. Установить на правило ключ фильтрации. Ключ фильтрации - это произвольная текстовая строка длиной не больше 31 символа. Ключ помогает

уникально идентифицировать записи, генерируемые в хода аудита за точкой наблюдения;

- -m текст. Послать в систему аудита пользовательское сообщение. Это возможно только из учетной записи root;
- -p [r|w|x|a]. Установить фильтр прав доступа для точки наблюдения. r=чтение, w=запись, x=исполнение, a=изменение атрибута;
- -r частота. Установить ограничение скорости выдачи сообщений в секунду (0 - нет ограничения). Если эта частота не нулевая, и она превышается в ходе аудита, флаг сбоя выставляется ядром для выполнения соответствующего действия. Значение по умолчанию: 0;
- -R AUDIфайл. Читать правила из файла. Правила должны быть расположены по одному в строке и в том порядке, в каком они должны исполняться. Следующие ограничения накладываются на файл: владельцем должен быть root, и доступ на чтение должен быть только у него;
- -s. Получить статус аудита;
- -a список, действие. Добавить правило с указанным действием к концу списка;
- -A список, действие. Добавить правило с указанным действием в начало списка;
- -d список, действие. Удалить правило с указанным действием из списка. Правило удаляется только в том случае, если полностью совпали имя системного вызова и поля сравнения;
- -D. Удалить все правила и точки наблюдения;
- -S [Имя или номер системного вызова|all]. Любой номер или имя системного вызова могут быть использованы. Также возможно использование ключевого слова all. Если какой-либо процесс выполняет указанный системный вызов, то аудит генерирует соответствующую запись. Если значения полей сравнения заданы, а системный вызов не указан, правило будет применяться ко всем системным вызовам. В одном правиле может быть задано несколько системных вызовов - это положительно сказывается на производительности, поскольку заменяет обработку нескольких правил;
- -F [n=v | n!=v | n<v | n>v | n<=v | n>=v | n&v | n&=v]. Задать поле сравнения для правила. Атрибуты поля следующие: объект, операция, значение. Можно задать до 64 полей сравнения в одной команде. Каждое новое поле должно начинаться с -F. Аудит будет генерировать запись, если произошло совпадение по всем полями

сравнения. Допустимо использование одного из следующих 8 операторов: равно, не равно, меньше, больше, меньше либо равно, больше либо равно, битовая маска (n&v) и битовая проверка (n&=v). Битовая проверка выполняет операцию 'and' над значениями и проверяет, равны ли они. Битовая маска просто выполняет операцию 'and'. Поля, оперирующие с идентификатором пользователя, могут также работать с именем пользователя - программа автоматически получит идентификатор пользователя из его имени. То же самое можно сказать и про имя группы:

- in_syscall: Состояния работы процесса в системном вызове или в прерывании;
- serial: уникальное число, помогающее идентифицировать определенную запись аудита. Вместе с ctime оно может определить, какие части принадлежат той же записи аудита. Данный набор (Метка времени и serial) уникален для каждого системного вызова, и он существует от начала системного вызова до выхода из него;
- ctime: Время входа в системный вызов;
- major: Номер системного вызова;
- массив argv: первые 4 параметра системного вызова;
- name_count: Количество имён. Определён максимум, равный 20;
- audit_names: массив структур audit_names, содержащих данные, скопированные getname();
- auditable: Если audit_context должен быть записан на выходе из системного вызова, то это поле устанавливается в 1;
- pwd: Текущий рабочий каталог, в котором запущена задача;
- pwdmnt: Текущая рабочая точка монтирования каталога. Pwdmnt и pwd используются для установки поля cwd (тип записи аудита FS_WATCH);
- aux: указатель на вспомогательную структуру данных, которая будет использоваться для специфической информации аудита;
- pid: идентификатор процесса;
- arch: архитектура;
- personality: индивидуальный номер ОС;
- другие поля: контекст аудита также содержит идентификаторы пользователя и группы реальные, действительные, ser и идентификатор файловой системы: uid, euid, suid, fsuid, gid, egid, sgid, fsgid;

- -w путь. Добавить точку наблюдения за файловым объектом, находящемся по указанному пути;

- -W путь. Удалить точку наблюдения за файловым объектом, находящемся по указанному пути;

Например, чтобы в журнале стали фиксироваться все системные вызовы, используемые определенным процессом (с идентификатором 1005), необходимо выполнить команду:

auditctl -a exit,always -S all -F pid=1005

Чтобы в журнале фиксировались все файлы, открытые определенным пользователем (с идентификатором 510), необходимо выполнить команду:

auditctl -a exit,always -S open -F auid=510 –F arch=b32

6.7 Приложение «Администрирование SELinux»

Для настройки механизмов аудита модуля политики SELinux предназначено приложение «Администрирование SELinux», которое запускается из меню «Система–> Администрирование–> Управление SELinux» и доступно только в режиме администратора.

В окне приложения «Администрирование SELinux» на вкладке «Модуль политики» включить аудит можно кнопкой «Включить аудит» (рис. 143).

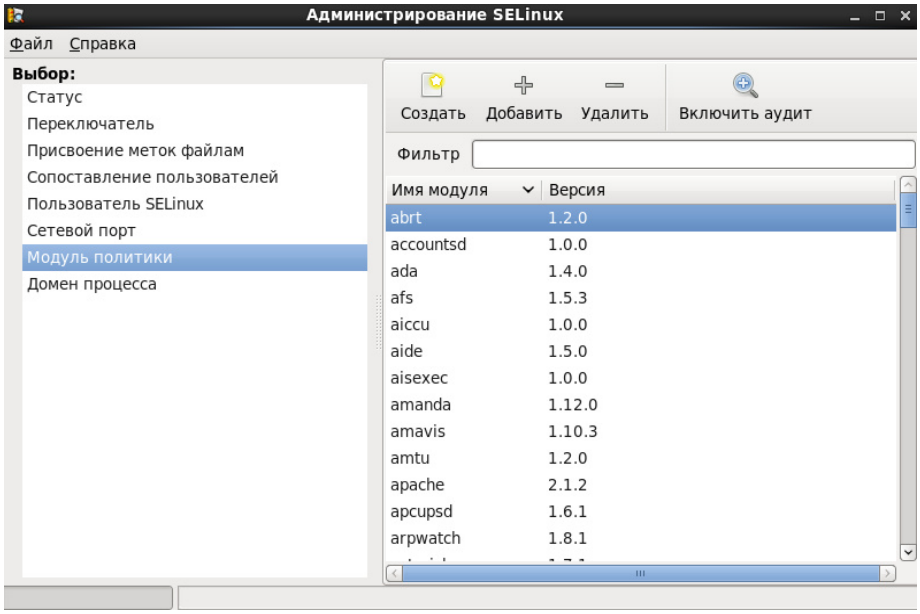


Рисунок 143 – Администрирование SELinux вкладка «Модуль политики»

6.8 Приложение "Audit Logs"

Для просмотра журналов аудита используется приложение "Audit Logs", которое запускается из главного меню "Система–>Администрирование–>Audit Logs".

"Audit Logs" позволяет администратору самому определить события безопасности, которые должны подлежать регистрации, определить состав и содержание информации.

При запуске "Audit Logs" отображается вкладка, представляющая собой таблицу журнала аудита с записями о действиях пользователя. Для работы с этой таблицей используется пункт меню "List–>Свойства". Во вкладке "General" окна "Propetries" (Свойства) можно задать название открытой вкладки, сортировку по времени происхождения события, порядок событий по убыванию или возрастанию (рис. 144).

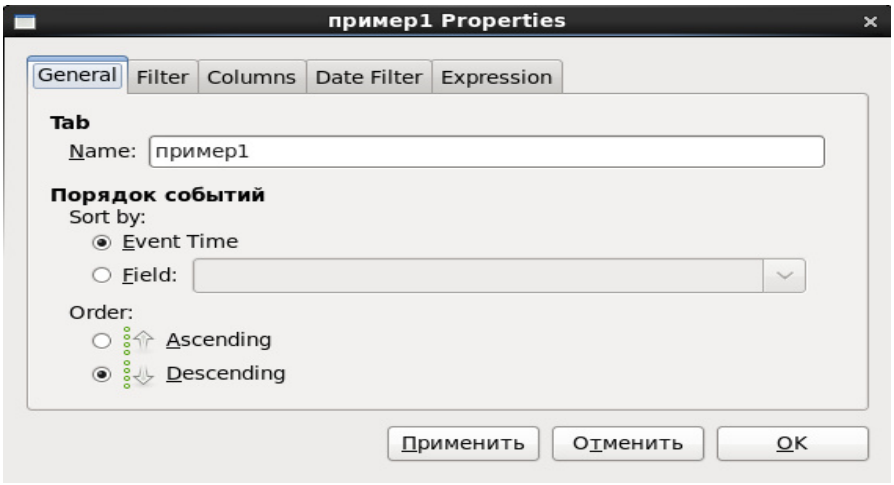


Рисунок 144 – Общая информация о таблице

Во вкладке «Filter» предлагается задать/исключить название события, чтобы в журнале отображались только интересующие вас типы изменений (рис. 145).

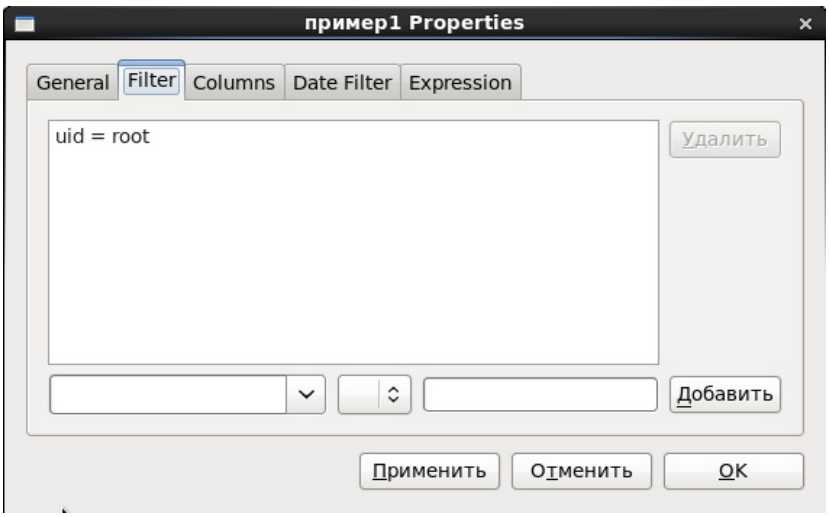


Рисунок 145 – Использование фильтра

Во вкладке «Columns» можно изменить для удобства порядок столбцов (первым столбцом может быть не дата, а событие или любой столбец, который захотите добавить) (рис. 146).

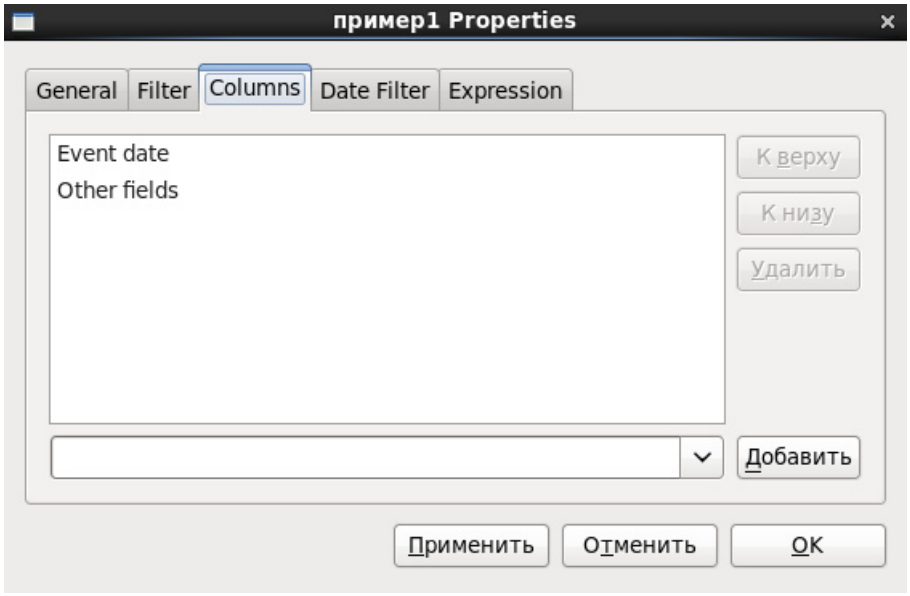


Рисунок 146 – Изменение порядка столбцов

Во вкладке "Date Filter" можно задать промежуток времени, по которому хотите увидеть отчетную таблицу (рис. 147).

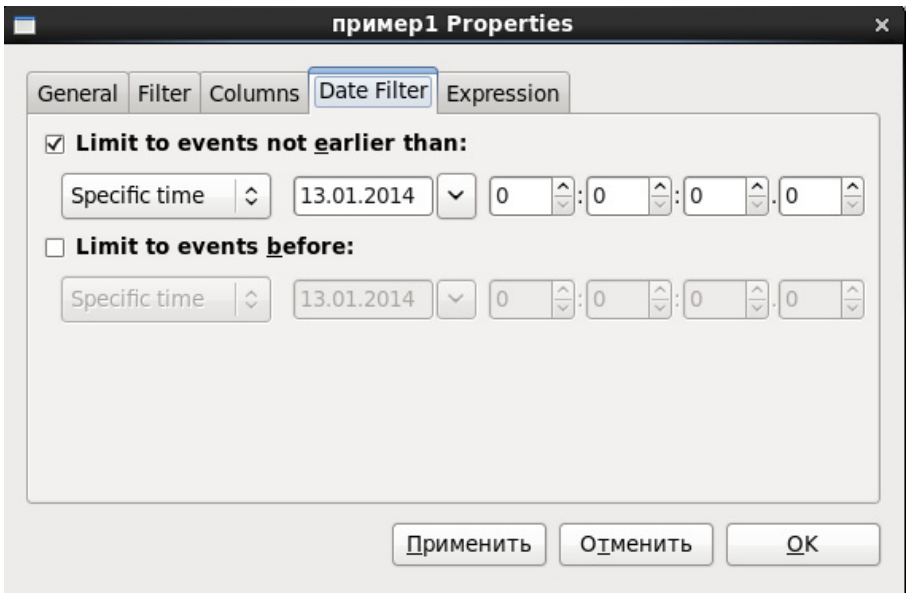


Рисунок 147 – Задать промежуток времени для фильтра

Изм.	Лист	№ докум	Подп	Дата

Чтобы увидеть детализацию события, необходимо выделить интересующую строку, кликнуть по ней 2 раза правой кнопкой мыши или выбрать в пункте меню выбрать "View"–> "Event Details" (рис. 148).

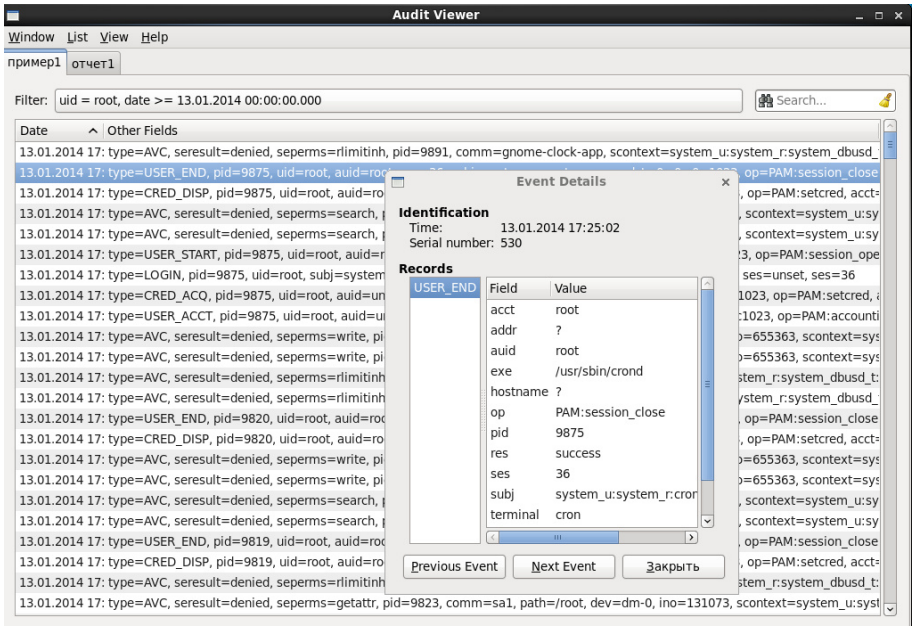
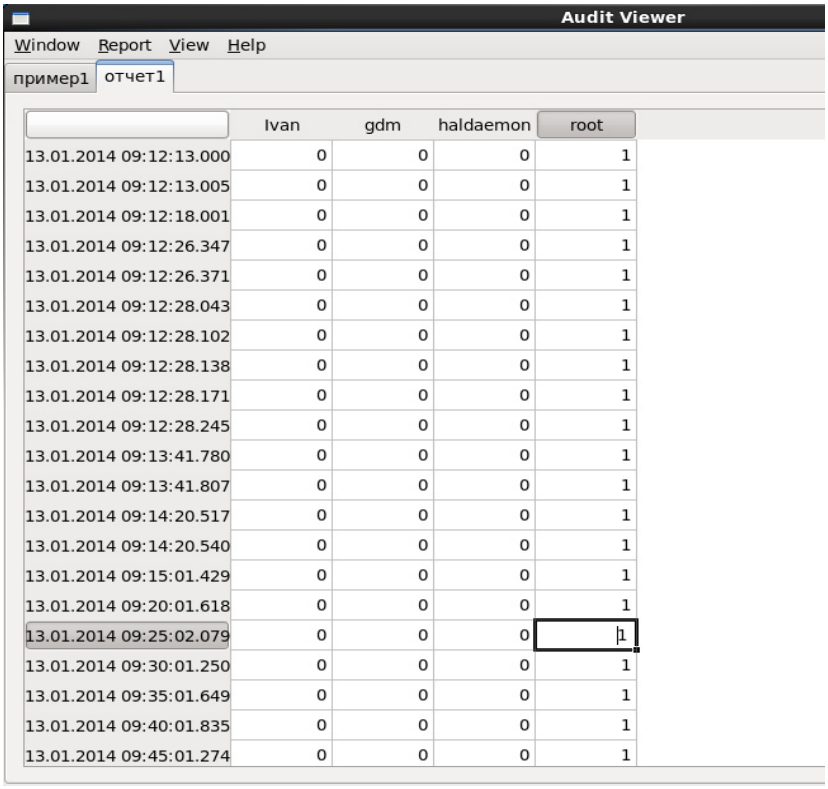


Рисунок 148 – Пример детализации события

Для создания отчета по интересующим событиям используется пункт меню "Window"–>"New Report". Свойства отчета схожи со свойствами таблицы (рис. 149).



	Ivan	gdm	haldaemon	root
13.01.2014 09:12:13.000	0	0	0	1
13.01.2014 09:12:13.005	0	0	0	1
13.01.2014 09:12:18.001	0	0	0	1
13.01.2014 09:12:26.347	0	0	0	1
13.01.2014 09:12:26.371	0	0	0	1
13.01.2014 09:12:28.043	0	0	0	1
13.01.2014 09:12:28.102	0	0	0	1
13.01.2014 09:12:28.138	0	0	0	1
13.01.2014 09:12:28.171	0	0	0	1
13.01.2014 09:12:28.245	0	0	0	1
13.01.2014 09:13:41.780	0	0	0	1
13.01.2014 09:13:41.807	0	0	0	1
13.01.2014 09:14:20.517	0	0	0	1
13.01.2014 09:14:20.540	0	0	0	1
13.01.2014 09:15:01.429	0	0	0	1
13.01.2014 09:20:01.618	0	0	0	1
13.01.2014 09:25:02.079	0	0	0	1
13.01.2014 09:30:01.250	0	0	0	1
13.01.2014 09:35:01.649	0	0	0	1
13.01.2014 09:40:01.835	0	0	0	1
13.01.2014 09:45:01.274	0	0	0	1

Рисунок 149 – Создание отчета

Изменить источник хранения событий можно с помощью пункта меню "Window" –> "Change event source", выбрав системную папку audit.log (рекомендуется) или произвольную папку (рис. 150).

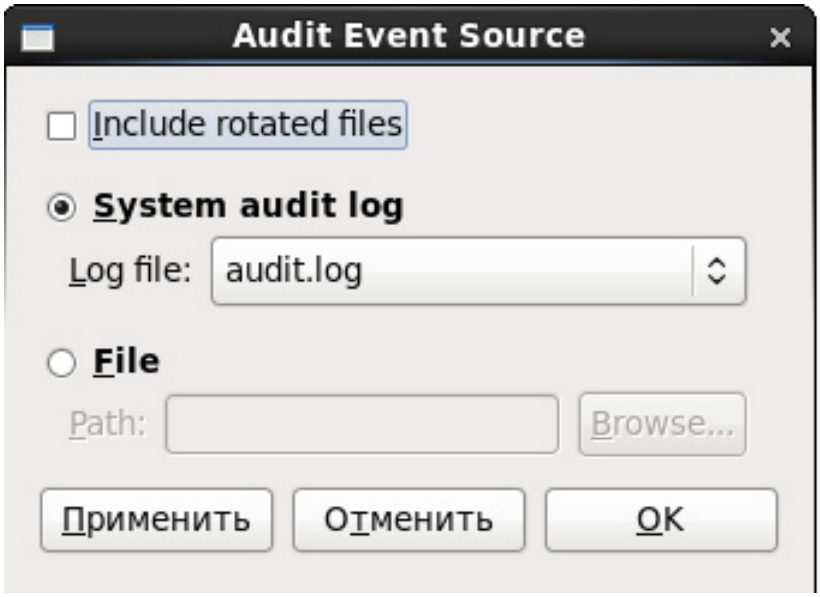


Рисунок 150 – Выбор источника хранения событий

Для экспорта созданного документа используйте вкладку "Report"–>"Export" (рис. 151).

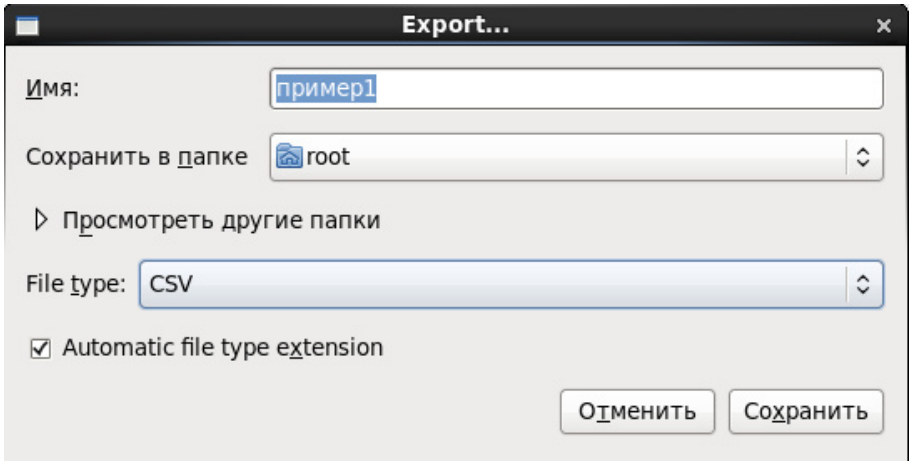


Рисунок 151 – Экспорт документа

Сохранить полученные отчеты можно с помощью "Window"–>"Save layout as" или "List"–>"Save Configyration as".

6.9 Приложение "KsystemLog"

Мониторинг (просмотр, анализ) результатов регистрации событий аудита осуществляется с помощью приложения "KsystemLog", которое запускается из главного меню "Приложения–> Системные–>KsystemLog".

"KsystemLog" поддерживает вкладки, которые открываются нажатием Ctrl+T или "окно" – "новая вкладка". Таким образом, можно просматривать несколько журналов одновременно в одном окне на разных вкладках.

6.10 Доступ к данным аудита

Доступ к данным аудита обычным пользователям запрещён, это ограничение наложено на доступ к журналу аудита и конфигурационным файлам аудита (они доступны только системному администратору).

Системный администратор может определить события аудита из всего набора событий с использованием простого фильтра LAF. Это обеспечивает гибкое определение событий аудита и условий, при которых выполняются события. Системный администратор может определить набор идентификаторов пользователей для аудита или, наоборот, набор идентификаторов пользователей, для которых аудит не будет выполняться.

7 ЗАЩИТА ОТ ВЫПОЛНЕНИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

7.1 Основные сведения

Средства защиты от выполнения вредоносного программного обеспечения МСВСфера 6.3 АРМ предоставляют следующие возможности:

- обеспечение безопасности физического доступа к компьютеру;
- доверенная загрузка операционных систем;
- парольная защита;
- защита учетных записей и административных прав;
- конфигурирование доступа к памяти, содержащей стек только на чтение и запись, но не исполнение программ;
- выполнение рандомизации адресного пространства, влияющее на позиции независимого кода библиотек (PIC), а также позиции независимых исполнимых программ (PIE);
- маркировка всех секций двоичного файла приложения перед загрузкой как доступных только для чтения, из исключением данных "кучи";
- блокирование сеанса пользователя по истечению времени бездействия;
- обеспечение надежных меток времени;
- анализ изменений системных файлов;
- анализ сетевого трафика.

Вышеперечисленные возможности защиты от выполнения вредоносного программного обеспечения реализуются с помощью следующих программных компонент:

- приложение "Настройка Kickstart";
- конфигурационный файл /boot/grub/grub.conf;
- приложение "Менеджер пользователей";
- конфигурационный файл /etc/sudoers;
- приложение "Настройка межсетевого экрана";
- приложение "Хранитель экрана";
- надежные метки времени;

- утилита AMTU;
- менеджер пакетов RPM;
- анализаторы трафика.

7.2 Приложение "Настройка Kickstart"

Физический доступ к компютеру и загрузка нештатных операционных систем, как возможные варианты несанкционированного доступа к компьютеру, предотвращаются с помощью настроек приложения "Настройка Kickstart" и конфигурационного файла /boot/grub/grub.conf, как описано в подразделе 4.11.

7.3 Встроенные средства и настройки

Система МСВСфера 6.3 АРМ включает средства защиты от выполнения вредоносного программного обеспечения, включенные в нее по умолчанию. К ним относятся:

1. Конфигурирование доступа к памяти, содержащей стек только на чтение и запись, но не исполнение программ. По умолчанию все процессы и потоки используют стек, который не может быть исполнимым.

2. Выполнение рандомизации адресного пространства, влияющей на позиции независимого кода библиотек (PIC), а также позиции независимых исполняемых программ (PIE). Все разделяемые библиотеки обязательно являются PIC библиотеками, а несколько отобранных приложений в системе являются PIE приложениями. Пользователи могут скомпилировать свои приложения как PIE для рандомизации адресного пространства этих приложений.

3. Маркировка всех секций двоичного файла приложения перед загрузкой как доступных только для чтения, за исключением данных "кучи". Эта поддержка работает для отобранных приложений в системе, и в частности, скомпилированных пользовательских приложений. Частичная защита также возможна, она подразумевает, что секция .got.plt маркируется доступной для чтения и записи.

7.4 Утилита sudo

Система МСВСфера 6.3 АРМ создана таким образом, чтобы рядовые пользователи не работали в системе под учетной записью root (суперпользователь, администратор). Благодаря этому программы и файлы не могут быть запущены на выполнение без явного предоставления полномочий. Поскольку без полномочий администратора запуск программ в таком режиме работы невозможен, вредоносное ПО не может самостоятельно инсталлировать себя или распространяться в системе. Система ограничения доступа и полномочий пользователей является одним из самых эффективных инструментов борьбы с распространением вредоносного программного обеспечения.

Настройка безопасности учетных записей в системе и административных прав описана в подразделах 4.4 и 4.7.

7.5 Приложение "Менеджер пользователей"

Одним из важнейших атрибутов безопасности учетной записи, предотвращающих вторжение, является пароль пользователя. Изменять свой собственный пароль пользователь может только в соответствии с правилами, предоставленными системой. Алгоритм md5 позволяет использовать более длинные пароли в системе, по сравнению с обычным ограничением в восемь символов. Система использует библиотеку pam_passwdqc.so, чтобы выполнять дополнительные проверки надежности пароля. Например, отклоняются такие пароли, как "1qaz2wsx", т.к. подобный пароль легко набрать на клавиатуре. В дополнение к проверке обычных паролей предлагается поддержка парольных фраз и генерация случайных паролей.

Во время инициализации сеанса пользователя подсистема идентификации и аутентификации обращается к базе данных /etc/security/opasswd, которая хранит определённое число X новых паролей. Они используются для смены пароля и хранят всю историю изменений, чтобы препятствовать использованию пользователем одних и тех же паролей (Remember = X; это - одна из опций, поддерживаемых pam_unix.so). Владельцем файла является root и группа root.

На практике обычно используются теневые пароли, и вместо пароля в файле /etc/passwd стоит *, а сам пароль хранится в файле /etc/shadow в зашифрованном виде. Применение теневых паролей оправдывает себя с точки зрения безопасности. Обычно к файлу /etc/passwd

разрешен доступ в режиме «только чтение» всем пользователям. К файлу /etc/shadow обычный пользователь не имеет даже такого доступа.

Все перечисленные способы парольной защиты существенно усложняют взлом пароля злоумышленником. Следует задавать более сложный пароль, особенно для административных и системных учетных записей.

Настройка парольной безопасности описана в подразделе 3.4.

7.6 Приложение "Настройка межсетевого экрана"

Для обеспечения безопасности системы используется брандмауэр (межсетевой экран). Брандмауэр устанавливается между вашим компьютером и сетью, ограничивая использование ресурсов вашего компьютера удалёнными пользователями сети. Правильно настроенный брандмауэр может сделать вашу систему более безопасной.

При использовании межсетевого экрана система не будет принимать не допущенные вами подключения, кроме разрешённых по умолчанию. По умолчанию разрешены только пакеты, отвечающие на исходящие запросы, например, ответы DNS или DHCP серверов. Если необходим доступ к службам, запущенным на этом компьютере, вы можете разрешить эти службы в брандмауэре. Например, вам могут понадобиться: SSH - набор инструментов для входа и выполнения команд с удалённой машины; протоколы HTTP и HTTPS, используемые Apache (и другими Web-серверами) для передачи web-содержимого; протокол FTP, используемый для передачи файлов между компьютерами в сети; почтовый сервер SMTP для доставки почты через брандмауэр.

Подробное описание настройки межсетевого экрана представлено в разделе 9.

7.7 Приложение "Хранитель экрана"

Для защиты от выполнения вредоносного программного обеспечения системой предусмотрено также блокирование сеанса пользователя по истечении времени бездействия посредством запуска приложения "Хранитель экрана", описание настройки и работы которого представлено в подразделе 4.9.

7.8 Надежные метки времени

Одной из уязвимостей механизма цифровой подписи (сообщений, файлов и другой информации) является возможность злоумышленной подделки меток времени на цифровых подписях и сертификатах ключей, например, путем изменения системных часов для генерации сертификатов открытых ключей и цифровых подписей, которые будут казаться созданными в иное, чем в действительности, время.

Одним из средств защиты от некорректной установки времени являются надежные метки времени. Метка времени удостоверяет время создания документа, дату использования электронной подписи, точное времени, когда документ поступил или получен.

Использование инструкций ввода/вывода для доступа к регистрам памяти CMOS, устанавливающим значение часов, осуществляется командой hwclock. Выполнив команду hwclock, получим значение аппаратных часов (рис.152).

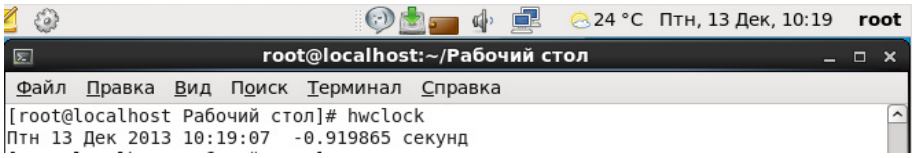


Рисунок 152 – Выполнение команды hwclock

Более подробная информация по утилите hwclock представлена в подразделе 5.25.

Каждый файл в системе ассоциирован с временной меткой, которая показывает время последнего доступа, последней модификации и последнего изменения файла. Чтобы узнать время создания, доступа или модификации файла, нужно запустить команду stat **<**имя_файла**>** (рис.153).

```
[root@localhost Рабочий стол]# stat Пример.txt
  File: «Пример.txt»
  Size: 0               Blocks: 0          IO Block: 4096   пустой обычный файл
Device: fd00h/64768d    Inode: 943150      Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2013-12-13 11:16:34.690676970 +0400
Modify: 2013-12-13 11:16:33.562579823 +0400
Change: 2013-12-13 11:16:33.562579823 +0400
```

Рисунок 153 – Выполнение команды stat для файла Пример.txt

Чтобы вручную изменить метку времени доступа к файлу на текущее время, нужно использовать ключ "-a" в команде touch, как на рис. 154.

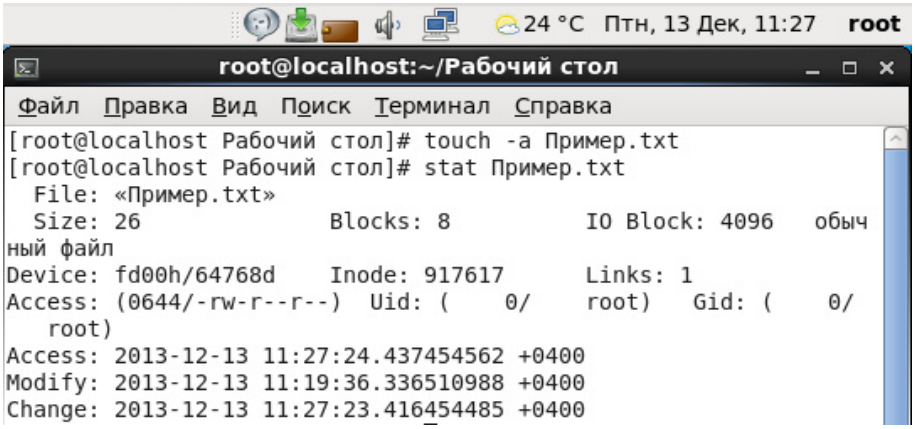


Рисунок 154 - Выполнение команды stat для файла Пример.txt

Чтобы вручную изменить время модификации файла на текущее время, нужно использовать ключ "-m" в команде touch, как на рис. 155.

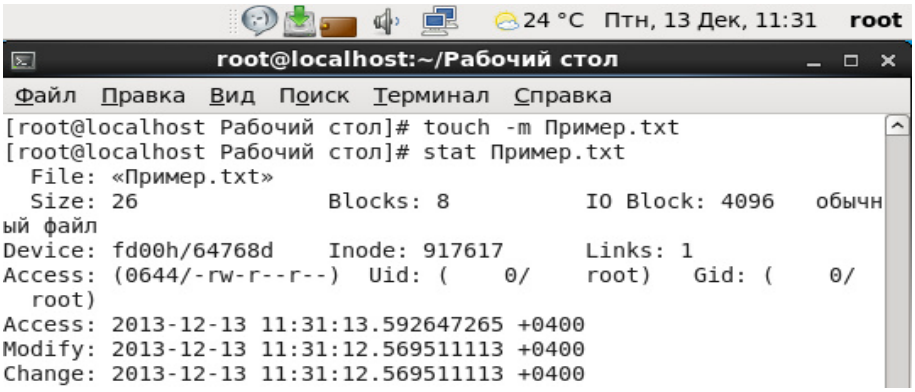


Рисунок 155 - Выполнение команды stat для файла Пример.txt

Чтобы задать явное значение меток, нужно использовать ключ "-d" в команде touch, например, как на рис. 156.

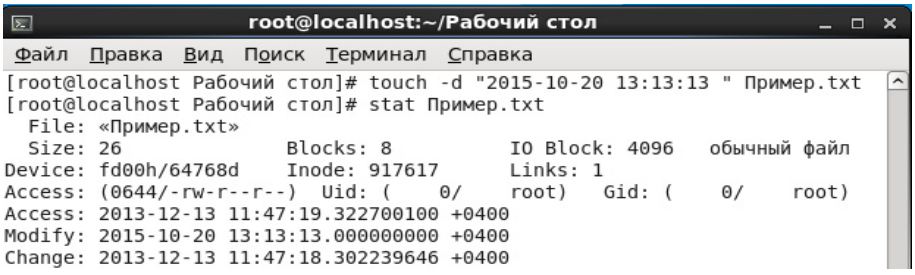


Рисунок 156 - Выполнение команды stat для файла Пример.txt

Чтобы скопировать метки времени с файла, нужно использовать ключ "-r" в команде touch, например, как на рис. 157 .

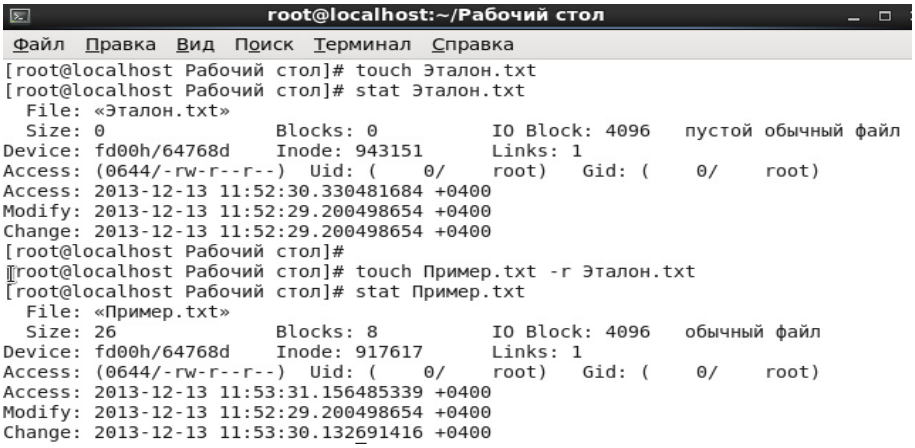


Рисунок 157 – Обновление меток времени файла Пример.txt

Приведенные примеры показывают, что при создании файла, изменении существующего файла или его атрибутов автоматически меняется временная метка файла, система предоставляет метки времени для собственного использования.

7.9 Утилита AMTU

МСВСфера 6.3 АРМ включает поддержку различных аппаратных архитектур и специальные средства тестирования функций используемого оборудования. Эти средства работают, предполагая, что они выполняются на некоторой абстрактной машине.

AMTU (абстрактная машинная тестовая утилита) - административная утилита, которая проверяет, выполняются ли основополагающие защитные механизмы.

Пример работы программы - вывода подсказок и выполнения теста памяти, приведен на рис. 158.

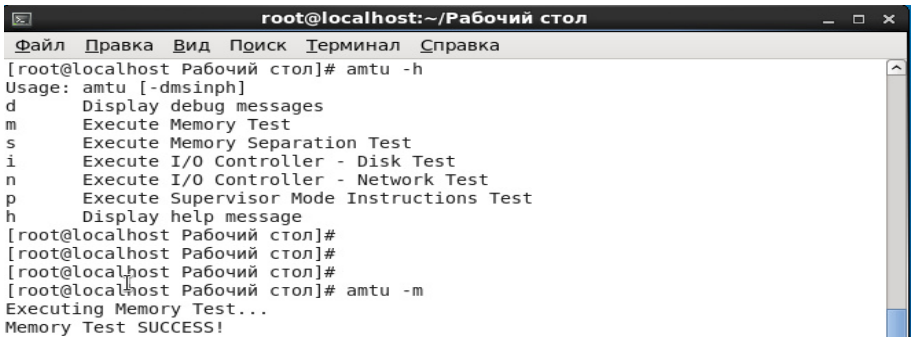


Рисунок 158 – Пример выполнения команд AMTU

Более подробная информация по механизму действия утилиты и использованию ее в системе представлена в подразделе 5.21.

7.10 Менеджер пакетов RPM

Важные системные файлы или программы могут быть изменены нежелательным образом. Для анализа изменений администратор может использовать менеджер пакетов RPM. Одной из полезных возможностей RPM является проверка системы на полноту. Если вам кажется, что вы удалили важный файл в каком-либо пакете, то проверьте его. Вы получите предупреждение, если в пакете чего-то не хватает. В этом случае вы можете легко реинсталлировать его. Любые измененные файлы конфигурации будут сохранены во время переустановки.

Проверка пакета сравнивает информацию о файлах, установленных из пакета, с информацией об оригинальных файлах пакета. Проверяется размер, контрольная сумма MD5, права доступа, тип, владелец и группа для каждого файла.

Команда rpm -V проверяет пакет. Вы можете использовать любые опции выбора пакетов, чтобы указать пакеты для проверки. Простейшее использование rpm -V foo, - которое проверяет, что все файлы пакета foo совпадают с теми, которые установлены в системе. Чтобы проверить все установленные пакеты, нужно использовать команду rpm -Va, как на рис. 159.

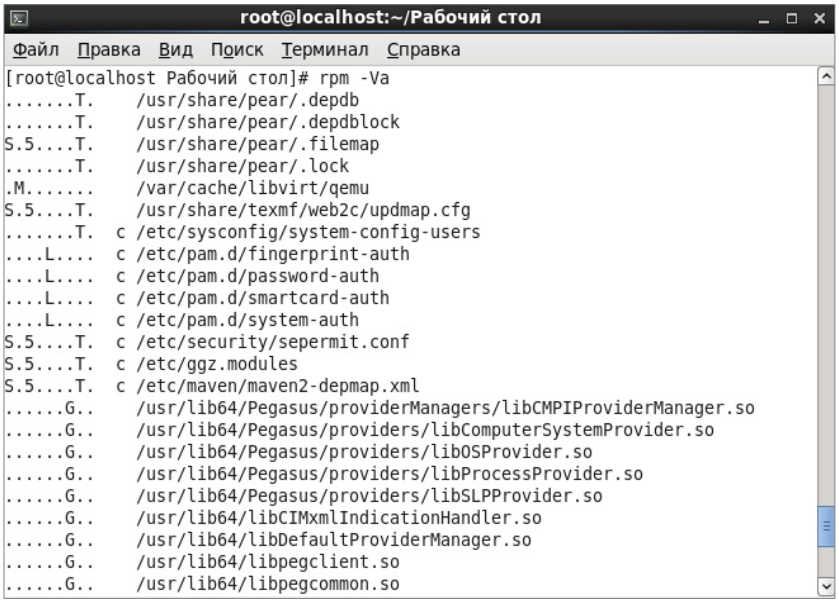


Рисунок 159 - Проверка установленных пакетов на полноту

Это может оказаться полезным, если вы подозреваете, что базы данных RPM повреждены.

Если сравнение произошло успешно, сигнализирующих об этом сообщений не будет выведено. Если же были найдены различия, они будут указаны. Формат вывода - строка из 8 символов, возможно с символом "c", обозначающим файл конфигурации, а затем имя файла. Каждый из 8 символов обозначает результат сравнения одного из атрибутов файла со значением атрибута в базе данных RPM. Знак "." (точка) означает, что тест пройден. Следующие символы обозначают ошибки в тестах:

5 - контрольная сумма MD5;

S - размер файла;

L - символическая ссылка;

T - время модификации файла;

D - устройство;

U - пользователь;

G - группа;

M - режим (включает права доступа и тип файла);

? - нечитаемый файл.

7.11 Анализаторы трафика

Для поиска и анализа подозрительной сетевой активности в системе могут использоваться анализаторы трафика. Анализатор трафика - это программа, предназначенная для прослушивания и последующего анализа сетевого трафика. Ее использование в некоторых случаях позволяет обнаружить выполнение вредоносного программного обеспечения.

Программа tcpdump - это утилита, позволяющая перехватывать и анализировать сетевой трафик, проходящий через компьютер, на котором запущена данная программа.

Для выполнения программы требуется наличие прав администратора и прямой доступ к устройству. Утилита tcpdump предназначена для отладки сетевых приложений и сетевой конфигурации в целом.

Программа состоит из двух основных частей: части захвата пакетов и части отображения захваченных пакетов, которая на уровне исходного кода является модульной, и для поддержки нового протокола достаточно добавить новый модуль.

Часть захвата пакетов при запуске передаёт «выражение выбора пакетов», идущее после всех параметров командной строки напрямую библиотеке захвата пакетов, которая проверяет выражение на синтаксис, компилирует его во внутренний формат данных, а затем копирует во внутренний буфер программы сетевые пакеты, проходящие через выбранный интерфейс и удовлетворяющие условиям в выражении.

Часть отображения пакетов выбирает захваченные пакеты по одному из буфера, заполняемого библиотекой, и выводит их в воспринимаемом человеком виде на стандартный вывод построчно в соответствии с заданным в командной строке уровнем детальности.

Если задан подробный вывод пакетов, программа проверяет, для каждого сетевого пакета имеется ли у неё модуль расшифровки данных, и, в случае наличия, соответствующей подпрограммой извлекает и отображает тип пакета в протоколе или передаваемые в пакете параметры.

Если tcpdump запустить без параметров, будет выведена информация обо всех сетевых пакетах, как на рис. 160.

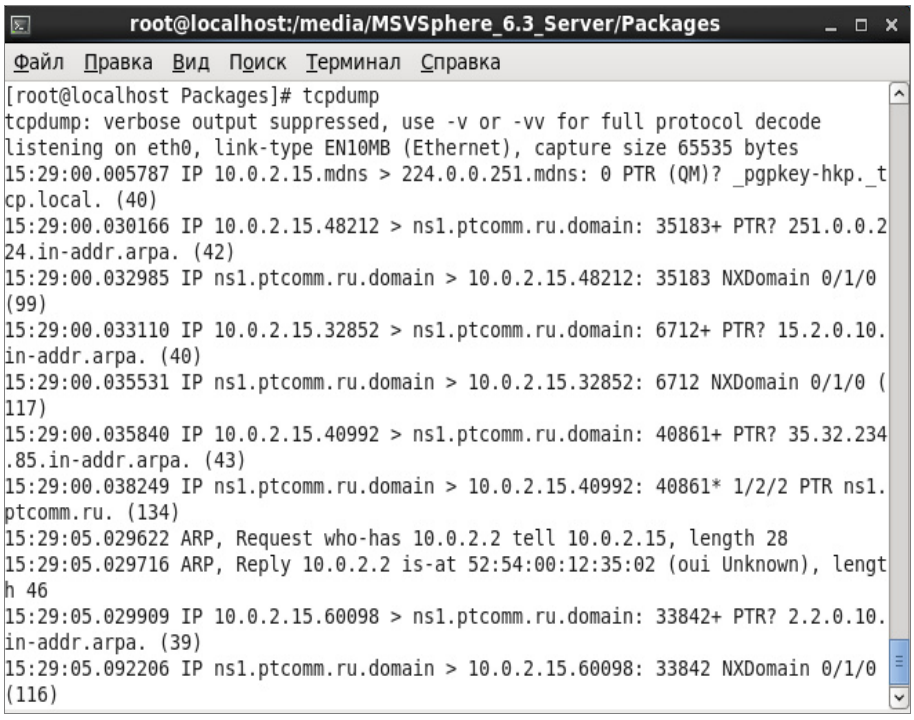


Рисунок 160 - Вывод информации о сетевых пакетах

С помощью параметра "-i" можно указать сетевой интерфейс, с которого следует принимать данные, например:

tcpdump -i eth2

Чтобы узнать получаемые или отправляемые пакеты от определенного хоста, необходимо его имя или IP-адрес указать после ключевого слова host:

tcpdump host nameofserver

Следующим образом можно узнать о пакетах, которыми обмениваются nameofserverA и nameofserverB:

tcpdump host nameofserverA and nameofserverB

Для отслеживания только исходящих пакетов от какого-либо узла нужно указать следующее:

tcpdump src host nameofserver

Только входящие пакеты:

tcpdump dst host nameofserver

Порт отправителя и порт получателя соответственно:

tcpdump dst port 80

tcpdump src port 22

Чтобы отслеживать один из протоколов TCP, UDP, ICMP, его название следует указать в команде. Использование операторов and (&&), or (||) и not (!) позволяет задавать фильтры любой сложности.

Пример фильтра, отслеживающего только UDP-пакеты, приходящие из внешней сети:

tcpdump udp and not src net localnet

Опции утилиты tcpdump:

-i <интерфейс> - задает интерфейс, с которого необходимо анализировать трафик;

-n - отключает преобразование IP в доменные имена, если указано "-nn", то запрещается преобразование номеров портов в название протокола;

-e - включает вывод данных канального уровня (например, MAC-адреса);

-v - вывод дополнительной информации (TTL, опции IP);

-s <размер> - указание размера захватываемых пакетов (по-умолчанию - пакеты больше 68 байт);

-w <имя_файла> - задать имя файла, в который сохранять собранную информацию;

-r <имя_файла> - чтение дампа из заданного файла;

-p - захватывать только трафик, предназначенный данному узлу (по умолчанию - захват всех пакетов, в том числе широковещательных);

-q - переводит tcpdump в "бесшумный режим", в котором пакет анализируется на транспортном уровне (протоколы TCP, UDP, ICMP), а не на сетевом (протокол IP);

-t - отключает вывод меток времени.

Функциональность, которую предоставляет tcpdump, очень схожа с возможностями программы Wireshark. Wireshark - программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других. Она имеет графический пользовательский интерфейс и вызывается из меню системы "Приложения->Интернет->Wireshark Network Analyzer" (рис. 161).

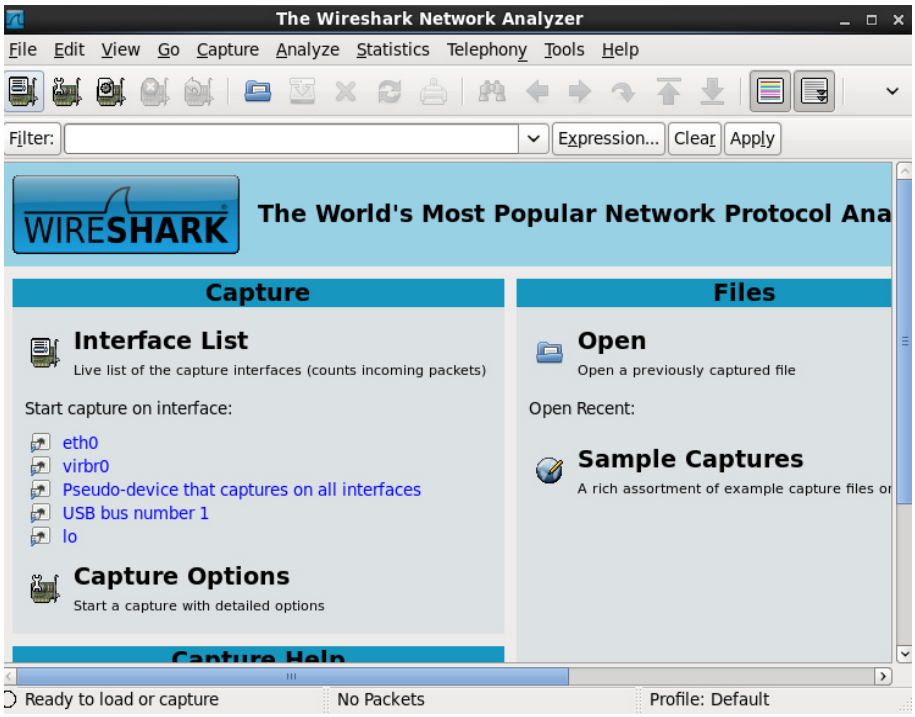


Рисунок 161 - Окно приложения "The Wireshark Network Analyzer"

Приложение Wireshark имеет гораздо больше возможностей по сортировке и фильтрации информации. Программа позволяет пользователю просматривать весь проходящий по сети трафик в режиме реального времени, переводя сетевую карту в так называемый неразборчивый режим (англ. promiscuous mode).

Wireshark - это приложение, которое знает структуру самых различных сетевых протоколов, умеет работать с множеством форматов входных данных и позволяет разобрать сетевой пакет, отображая значение каждого поля протокола любого уровня.

Для начала сборки перехваченных программой пакетов сообщений по сети выберите пункт главного меню "Capture->Interfaces" или кнопку на верхней панели инструментов "List the available capture interfaces" – после этого на экране появится диалоговое окно, как на рис. 162.

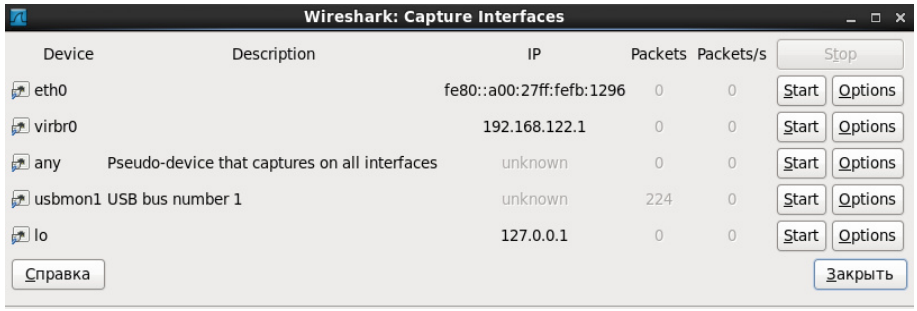


Рисунок 162 - Окно настройки интерфейсов

С помощью кнопки "Options" возможна установка желаемых параметров работы программы (рис. 163). В открывшемся окне настройки разделены на пять областей: "Capture" (Захват), "Capture File(s)" (Захват файлов), "Stop Capture..." (Остановить захват), "Display Options" (Показать настройки), "Name Resolution" (Разрешение имен).

В области "Capture" нужно указать название интерфейса (Interface), тип заголовка канального уровня (Link-layer header type), по умолчанию Ethernet. Если необходимо, выбрать захват пакетов в беспорядочном режиме (Capture packets in promiscuous mode), захват пакетов в pcap-ng экспериментальном формате (Capture packets in pcap-ng format (experimental)), ограничение каждого пакета в байтах (Limit each packet to ... bytes). Так же можно указать фильтр захвата (Capture Filter).

В области "Capture File(s)" нужно указать путь к файлу (File), установить галочку на использование нескольких файлов (Use multiple files). Если использована опция "Use multiple files", то нужно указать еще ограничение в мегабайтах или минутах для каждого следующего файла (Next file every), количество файлов для кольцевого буфера (Ring buffer with ... files), количество файлов, после которых захват будет остановлен (Stop capture after ... file(s)).

В области "Stop Capture..." нужно указать ограничение в количестве пакетов (... after packet(s)), мегабайт (... after megabyte(s)) и минут (... after minute(s)).

В области "Display Options" нужно выбрать, нужны ли следующие опции: обновление списка пакетов в режиме реального времени (Update list of packets in real time), автоматическая прокрутка во время захвата (Automatic scrolling in live capture), скрыть информационный диалог о захвате (Hide capture info dialog).

В области "Name Resolution" нужно указать, будут ли использоваться следующие опции: включить разрешение MAC имени (Enable MAC name resolution), включить разрешение имен сети (Enable network name resolution), включить разрешение транспортных имен (Enable transport name resolution).

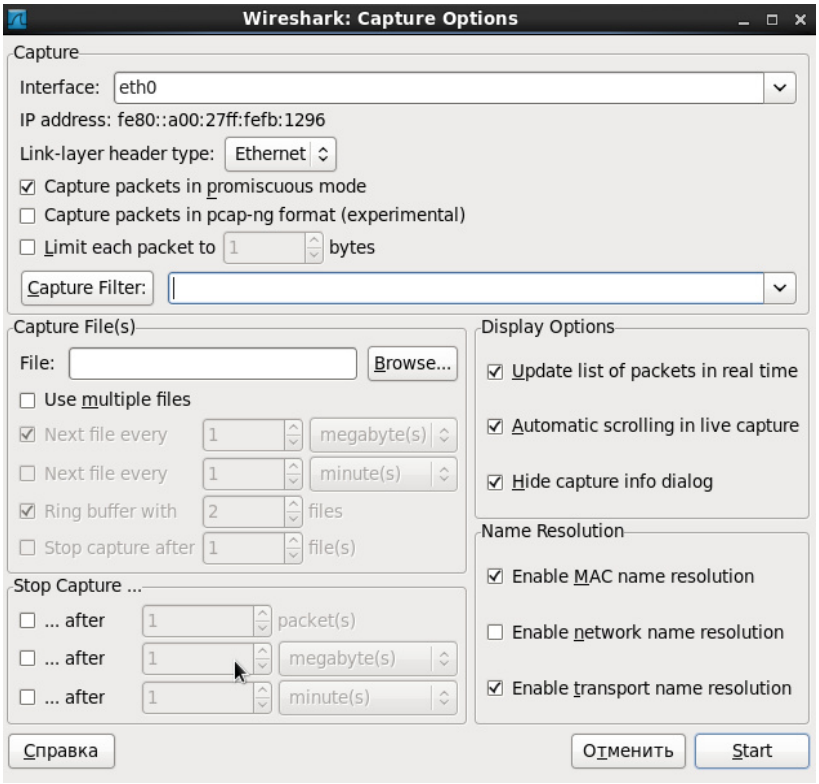


Рисунок 163 - Окно настройки параметров работы программы

Выберем интерфейс eth0. Для того чтобы начать процедуру захвата, необходимо нажать кнопку Start, после чего интерфейс программы примет вид, как на рис. 164. Для выбора настроек интерфейса нужно выбрать пункт меню "Capture->Options", для остановки захвата "Capture->Stop", для перезапуска - "Capture->Restart", для фильтрации запроса - "Capture->Capture Filters...".

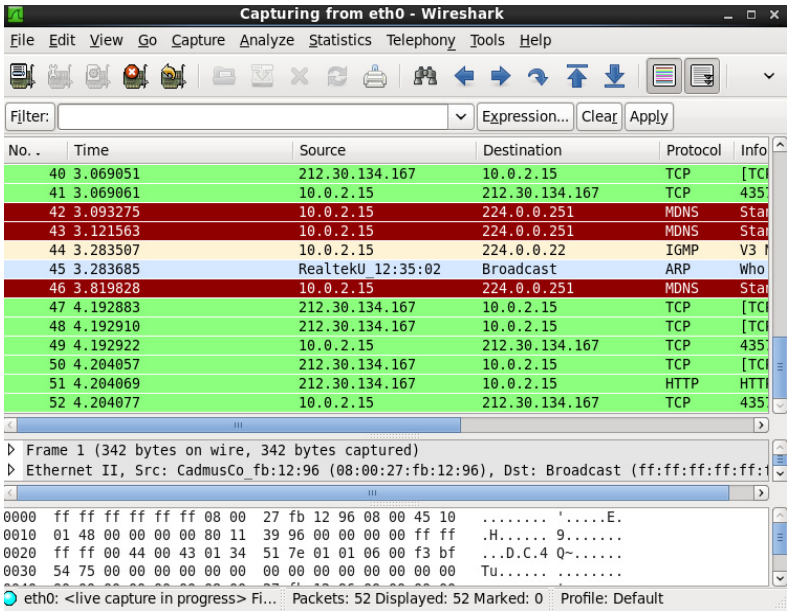


Рисунок 164 - Захват пакетов для интерфейса eth0

На рис. 164 видно, что окно Wireshark включает в себя три области просмотра с различными уровнями детализации. Верхнее окно содержит список собранных пакетов с кратким описанием, в среднем окне показывается дерево протоколов, инкапсулированных в кадр. Ветви дерева могут быть раскрыты для повышения уровня детализации выбранного протокола. Последнее окно содержит дамп пакета в шестнадцатеричном или текстовом представлении.

В верхней области данные разделены на шесть колонок – номера пакета в списке собранных, временная метка, адреса и номера портов отправителя и получателя, тип протокола и краткая информация о пакете.

Выбрав необходимый пакет из списка, мы можем просмотреть содержимое средней панели. В ней представлено дерево протоколов для пакета. Дерево отображает каждое поле и его значение для заголовков всех протоколов стека.

В программе Wireshark можно выбрать фильтрацию списка пакетов по IP-адресам, кликнув правую кнопку мыши, в контекстном меню нажать "Conversation filter->IP" (рис. 165).

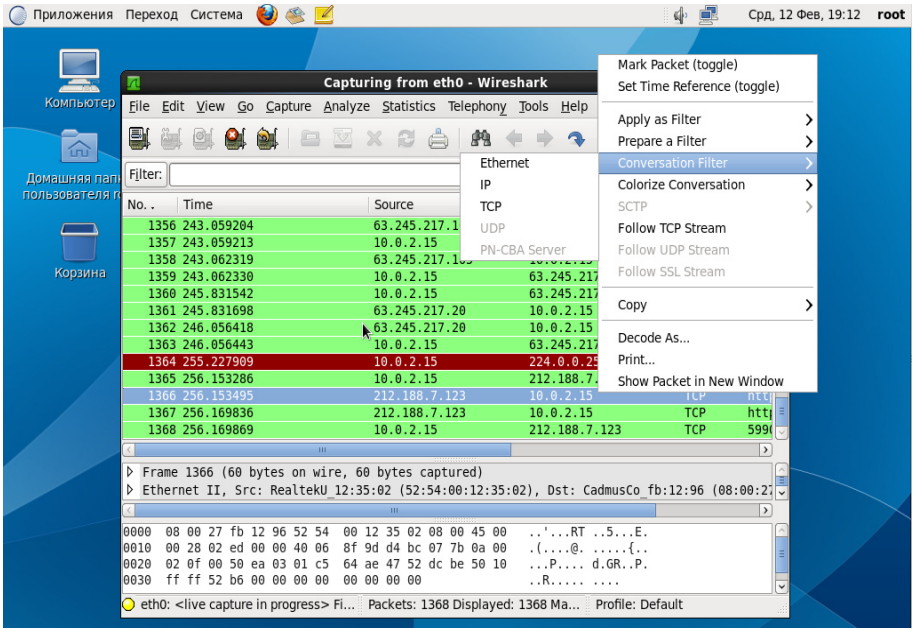


Рисунок 165 - Фильтрация пакетов

В результате получим окно, как на рис. 166, с отфильтрованными пакетами.

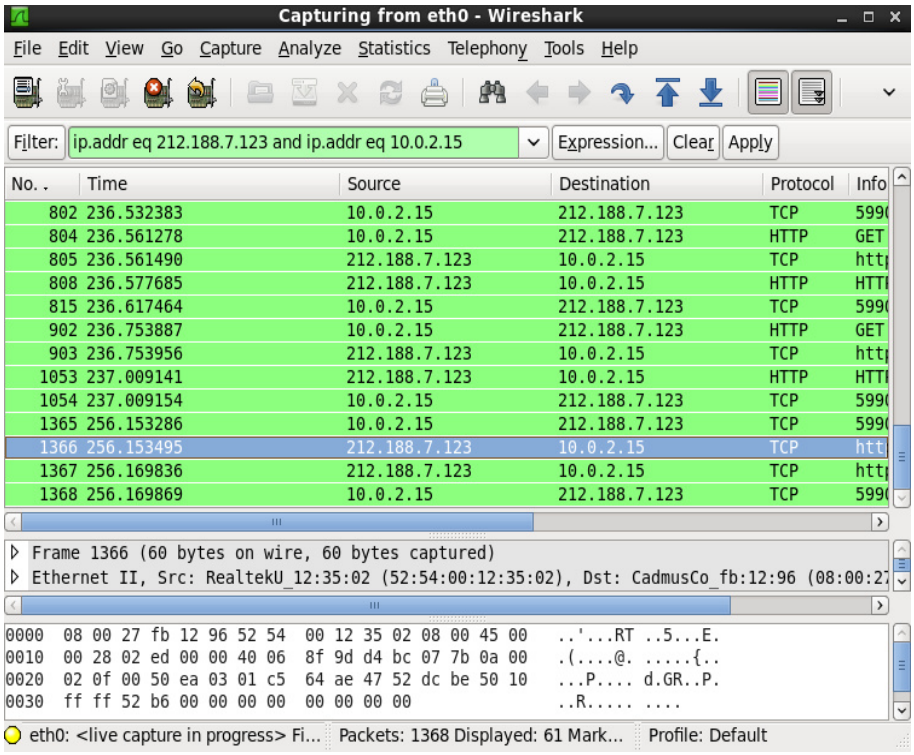


Рисунок 166 - Результат фильтрации по IP

Изм.	Лист	№ докум	Подп	Дата

Для того чтобы найти пакет среди общего списка, нужно выбрать пункт меню "Edit->Find Packet..." (рис. 167). Выбрать предмет поиска: показать фильтр (Display filter), шестнадцатиричное значение (Hex value) или строка (String) и указать сам фильтр.

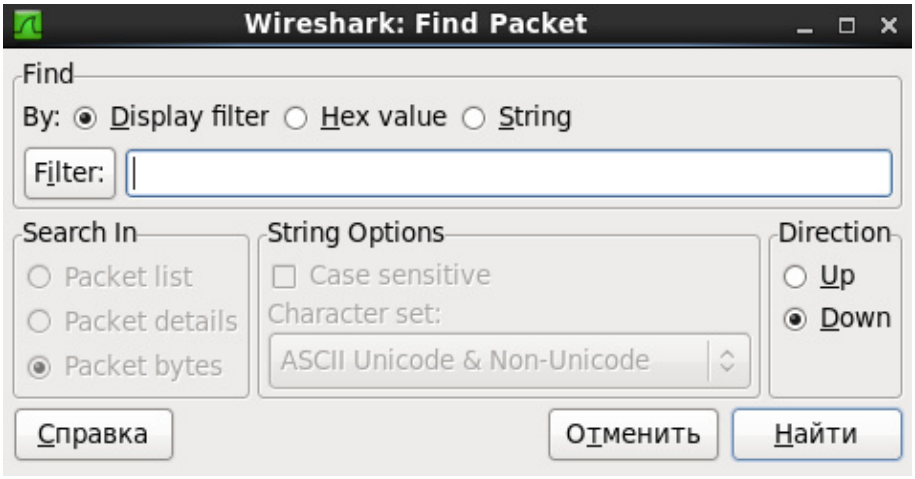


Рисунок 167 - Параметры поиска пакета

Wireshark предоставляет возможность сохранять файлы данных на жесткий диск. Для этого необходимо в главном меню программы выбрать "File->Export" и вариант сохранения данных (рис. 168). Например, если продолжить сохранение объекта HTTP - "Objects->HTTP", то можно сохранить объекты, найденные в Интернете, выбрав в появившемся списке "HTTP object list" необходимый файл и нажав "Save As" сохранить на диск.

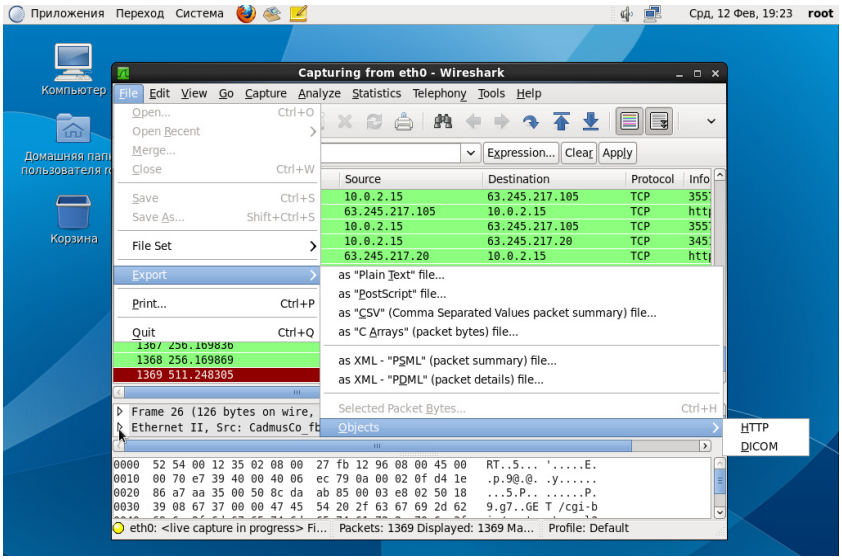


Рисунок 168 - Экспорт в файл

Изм.	Лист	№ докум	Подп	Дата

Программа обладает большим набором вывода статистических данных о захваченных пакетах сообщений. Так можно вывести общую таблицу иерархии протоколов при помощи пункта главного меню "Statistics>Protocol Hierarchy" (рис. 169).

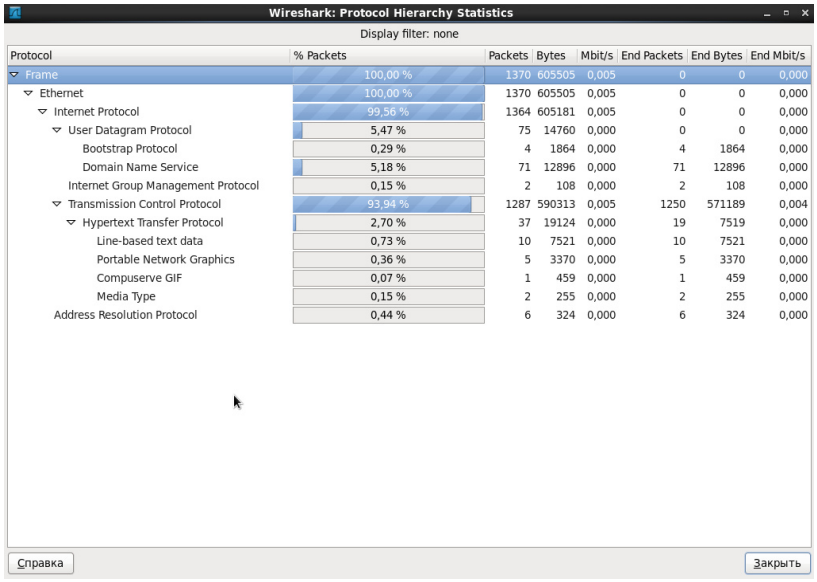


Рисунок 169 - Общая таблица иерархии протоколов

Для наглядного представления результатов выполнения захвата пакетов и сборки кадров в программе имеется возможность отображения данной информации в виде графика передачи пакетов в единицу времени. Для отображения данного графика необходимо воспользоваться пунктом главного меню "Statistics>IO Graphs".

Более подробную информацию о возможностях программы Wireshark можно найти на ее официальном сайте.

8 ЗАЩИТА СРЕДЫ ВИРТУАЛИЗАЦИИ

8.1 Основные сведения

Средства защиты среды виртуализации МСВСфера 6.3 АРМ предоставляют следующие возможности:

- идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре;
- управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин;
- регистрация событий безопасности в виртуальной инфраструктуре;
- управление потоками информации между компонентами виртуальной инфраструктуры;
- доверенная загрузка серверов виртуализации, виртуальной машины, серверов управления виртуализацией;
- управление перемещением виртуальных машин и обрабатываемых на них данных;
- контроль целостности виртуальной инфраструктуры и ее конфигураций;
- резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а так же каналов связи внутри виртуальной инфраструктуры;
- реализация и управление защитой от вредоносного программного обеспечения в виртуальной инфраструктуре;
- разбиение виртуальной инфраструктуры на сегменты для обработки информации отдельным пользователем и (или) группой пользователей.

Вышеперечисленные возможности защиты среды виртуализации реализуются с помощью следующих программных компонент:

- утилита virsh;
- утилита qemu-img;
- утилита ls;
- утилита iptables;

- утилита ip;
- утилиты getfattr и setfattr;
- подсистема sVirt;
- приложение "Конфигурация аутентификации".

8.2 Утилита virsh

Управление виртуальными машинами может осуществляться с помощью программной библиотеки (пакета) libvirt.

Установка пакета libvirt осуществляется командами в консоли:

yum install libvirt

yum install libvirt-client

Для нормальной работы libvirt необходимо сделать симлинк и перезагрузиться с помощью команд:

ln -s /usr/libexec/qemu /usr/bin/qemu

reboot

Запустить сервис libvirt можно с помощью команды:

/etc/init.d/libvirtd start

Сгенерировать xml-конфиг для libvirt на основе опций запуска qemu можно с помощью следующей команды:

virsh domxml-from-native qemu-argv vm.sh > vm.xml

При этом файл vm.sh может иметь вид:

```
/usr/bin/qemu -monitor stdio -m 512 -vga cirrus -localtime -cdrom i.iso -hda hda.qcow2 -net nic,vlan=0 , macaddr=DE:AD:BE:EF:00:00,model=e1000 -net bridge,vlan=0 -boot d -name "qmachine"
```

Полученный vm.xml будет иметь вид:

```
<domain type='qemu'>
  <name>qmachine</name>
  <uuid>4df7a085-2e89-0bed-9adf-52b4a84e85c0</uuid>
  <memory unit='KiB'>524288</memory>
  <currentMemory unit='KiB'>524288</currentMemory>
  <vcpu placement='static'>1</vcpu>
  <os>
    <type arch='i686'>hvm</type>
    <boot dev='cdrom'/>
```

```
  </os>
  <features>
    <acpi/>
  </features>
  <clock offset='localtime'/>
  <on_poweroff>destroy</on_poweroff>
  <on_reboot>restart</on_reboot>
  <on_crash>destroy</on_crash>
  <devices>
    <emulator>/usr/bin/qemu</emulator>
    <disk type='file' device='cdrom'>
      <source file='i.iso'/>
      <target dev='hdc' bus='ide'/>
      <readonly/>
      <address type='drive' controller='0' bus='1' target='0' unit='0'/>
    </disk>
    <disk type='file' device='disk'>
      <source file='hda.qcow2'/>
      <target dev='hda' bus='ide'/>
      <address type='drive' controller='0' bus='0' target='0' unit='0'/>
    </disk>
    <controller type='ide' index='0'/>
    <interface type='ethernet'>
      <mac address='de:ad:be:ef:00:00'/>
      <model type='e1000'/>
    </interface>
    <input type='mouse' bus='ps2'/>
    <graphics type='sdl'/>
    <video>
      <model type='cirrus' vram='9216' heads='1'/>
    </video>
    <memballoon model='virtio'/>
  </devices>
</domain>
```

Сгенерировать команду запуска виртуальной машины напрямую можно следующей командой:

virsh domxml-from-native qemu-argv vm.xml > vm.sh

Добавить xml-конфиг виртуальной машины в libvirt можно с помощью команды:

virsh define vm.xml

Запустить домен виртуальной машины можно командой:

virsh start qmachine

Уничтожить домен виртуальной машины и саму виртуальную машину соответственно можно с помощью операции:

virsh destroy qmachine

Просмотреть доступные домены виртуальных машин можно, выполнив команду:

virsh list --all

Получить список запущенных виртуальных машин можно, выполнив команду:

virsh -c qemu:///system list

Состояние виртуальной машины может быть сохранено в файл с целью возможного восстановления в дальнейшем. Приведенная команда сохранит состояние виртуальной машины в файл с именем, содержащим дату (где web_devel нужно заменить на соответствующее название виртуальной машины, а web_devel-022708.state **-** на описательное имя файла):

virsh -c qemu:///system save web_devel web_devel-022708.state

Сохраненная виртуальная машина может быть восстановлена командой:

virsh -c qemu:///system restore web_devel-022708.state

Выключить виртуальную машину:

virsh -c qemu:///system shutdown web_devel

Устройство CD-ROM может быть подмонтировано к виртуальной машине следующей командой: virsh -c qemu:///system attach-disk web_devel /dev/cdrom /media/cdrom

8.3 Утилита qemu-img

Утилита предназначена для преобразования форматов. С ее помощью следует выполнять форматирование виртуализированных гостевых систем, дополнительных устройств хранения и сетевых хранилищ.

Создать образы виртуальных машин QEMU можно командой в консоли:

qemu-img create -f qcow2 -o preallocation=metadata /path/to/hdd.qcow2 20G

Чтобы преобразовать образ диска QEMU из одного формата в другой, введем команду в консоль:

qemu-img convert –f cow cowimage.cow image.raw

Опция info утилиты qemu-img позволяет получить сведения о дисковом образе, пример команды:

qemu-img info –f cow cowimage.cow

8.4 Утилита ls

Все файлы образов виртуальных дисков для виртуальных машин лежат в /var/lib/libvirt/images (QEMU-образы или образы от других систем виртуализации, работающих под управлением libvirt). Файлам присвоены метки (пользователь:роль:тип): system_u:object_r:virt_image_t, для просмотра нужно ввести команду в консоли ls -Z**,** как на рис. 170. Из рисунка видны права доступа к файлам (-rw-r--r--) и владелец - системный пользователь (system_u).

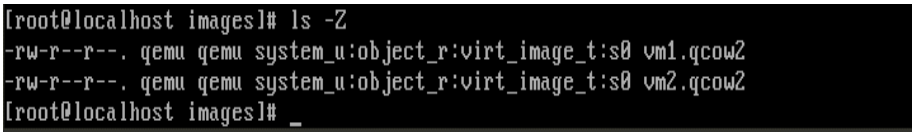


Рисунок 170 - Просмотр меток файлов

8.5 Утилита iptables

IPTables - утилита командной строки, которая является стандартным интерфейсом управления работой межсетевого экрана (брандмауэра) NETFilter.

Выключить службу iptables можно командой в консоли:

/etc/init.d/iptables stop

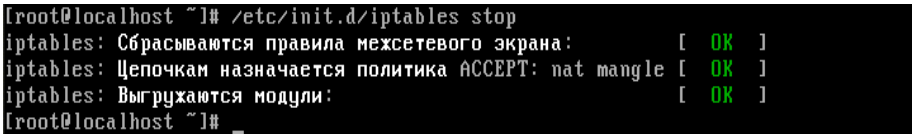


Рисунок 171 - Выключение службы iptables

Сброс (удаление) всех правил из заданной цепочки (если имя цепочки и таблицы не указывается, то удаляются все правила во всех цепочках) выполняется командой:

iptables -F

Команда iptables используется с набором ключей. Ключ -A добавляет новое правило в конец заданной цепочки, ключ -t указывает на используемую таблицу, ключ -o задает имя выходного интерфейса, ключ -j указывает действие над пакетом, ключ -I вставляет новое правило в цепочку, ключ -i указывает интерфейс, с которого был получен пакет, ключ -m загружает расширения, ключ --state проверяет признак состояния соединения. Примером

использования этих ключей для настройки iptables на host-системе может быть следующмй набор команд:

iptables -t nat -A POSTROUTING -o wlan0 -j MASQUERADE

iptables -I FORWARD 1 -i tap0 -j ACCEPT

iptables -I FORWARD 1 -o tap0 -m state --state RELATED,ESTABLISHED -j ACCEPT

Настройка iptables на host-системе, чтобы host стал шлюзом во внешнюю сеть для виртуальной машины, выполняется командами в консоли (рис. 172):

```
[root@localhost ~]# echo 1 > /proc/sys/net/ipv4/ip_forward
[root@localhost ~]# iptables -F
[root@localhost ~]# iptables -t nat -A POSTROUTING -o eth14 -j MASQUERADE
[root@localhost ~]# iptables -I FORWARD 1 -i tap0 -j ACCEPT
[root@localhost ~]# iptables -I FORWARD 1 -o tap0 -m state --state RELATED,ESTAB
LISHED -j ACCEPT
[root@localhost ~]#
```

Рисунок 172 - Настройка iptables на host-системе

8.6 Утилита ip

Утилита ip позволяет выполнять настройку сетевой подсистемы.

Для выполнения какой-либо операции после команды ip указывается объект и команда (возможно с аргументами), которая должна быть выполнена для этого объекта.

В качестве объектов можно указывать значения link, addr (адреса сетевых интерфейсов), route (маршруты), rule (правила), neigh, ntable, tunnel (тоннели), maddr, mroute, monitor, xfrm. Вместо полного имени объекта можно указывать только первые буквы, если это не вызывает неоднозначность.

Выполнить просмотр списка доступных сетевых карт командой можно в консоли ip addr (рис. 173).

```
[root@localhost ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth15: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN qlen 1000
    link/ether de:ad:cb:0f:15:0a brd ff:ff:ff:ff:ff:ff
3: eth14: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN qlen 1000
    link/ether de:ad:71:0f:15:14 brd ff:ff:ff:ff:ff:ff
4: virbr0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOW
N
    link/ether 52:54:00:d5:83:7f brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
5: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN qlen 500
    link/ether 52:54:00:d5:83:7f brd ff:ff:ff:ff:ff:ff
[root@localhost ~]#
```

Рисунок 173 - Просмотр списка доступных сетевых карт

Выставить IP-адрес сетевой карте, которая подключена к внешней сети, и задать маршрут шлюза по умолчанию для всех сетевых устройств в системе можно с помощью команд в консоли:

ip addr add 192.168.10.211/24 broadcast 192.168.10.255 dev eth0

ip link set eth0 up

ip route add via 192.168.10.1 dev eth0 metric 4

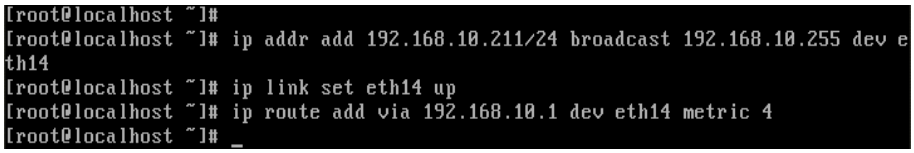


Рисунок 174 - Настройка сетевой карты и маршрута шлюза

8.7 Утилиты getfattr и setfattr

getfattr и setfattr - набор утилит для работы с расширенными атрибутами объектов файловой системы.

Выполнить экспорт атрибутов от всех файлов, расположенных в директории (рекурсивно) в отдельный файл можно с помощью следующих команд:

getfattr -Rd -m "-*" testfile > ../xattr_dump

cat ../xattr_dump

Выполнить импорт атрибутов из дампа можно с помощью команды:

setfattr —restore=./xattr_dump

8.8 Подсистема sVirt

С целью минимизации рисков безопасности, связанных с использованием подсистемы виртуализации, МСВСфера 6.3 АРМ содержит подсистему sVirt. Проект sVirt, базируется на SELinux и обеспечивает возможность настройки доступа виртуальных машин к разделяемым ресурсам. sVirt обеспечивает создание уникального ограниченного домена, которому запрещено общаться с другими доменами посредством подсистем SELinux. Использование ограниченного домена позволяет изолировать процессы гостевой ОС от возможности доступа к другим гостевым ОС или к родительской ОС.

Подсистема sVirt использует МАС для виртуальных машин и интегрируется в существующую структуру безопасности, обеспечиваемую подсистемой SELinux. Основной

целью sVirt является защита хоста и гостевых ОС от атак с использованием уязвимостей гипервизора. sVirt расширяет возможности SELinux, рассматривая каждую гостевую ОС как процесс, что позволяет использовать для них политики SELinux при настройке доступа к ресурсам.

Для настройки подсистемы виртуализации с использованием sVirt и libvirt определены флаги SELinux, приведенные в таблице 2.

Таблица 2. Флаги SELinux для виртуализации

Флаг SELinux	Описание
virt_use_comm	Разрешает использовать COMM-порт
virt_use_fusefs	Разрешает использовать файлы, примонтированные с использованием FUSE
virt_use_nfs	Разрешает управление NFS
virt_use_samba	Разрешает управление CIFS
virt_use_sanlock	Разрешает гостевой ОС взаимодействовать с sanlock
virt_use_sysfs	Разрешает настраивать PCI-устройств
virt_use_usb	Разрешает использование USB-устройств
virt_use_xserver	Разрешает взаимодействие с X Window System

Подобно другим сервисам, защищаемым SELinux, sVirt использует механизмы, основанные на процессах, назначенных метках и правах. Метки и права к ресурсам, используемым виртуальной машиной, назначаются динамически, а также, в случае необходимости, могут назначаться администратором статически. Динамический тип безопасности SELinux используется по умолчанию и предписывает libvirt выбирать уникальную метку для процесса и образа гостевой ОС, обеспечивая полную ее изоляцию.

Выбор типа назначения меток (динамический или статический) может быть выполнен, например, с помощью менеджера виртуальных машин при создании гостевой ОС.

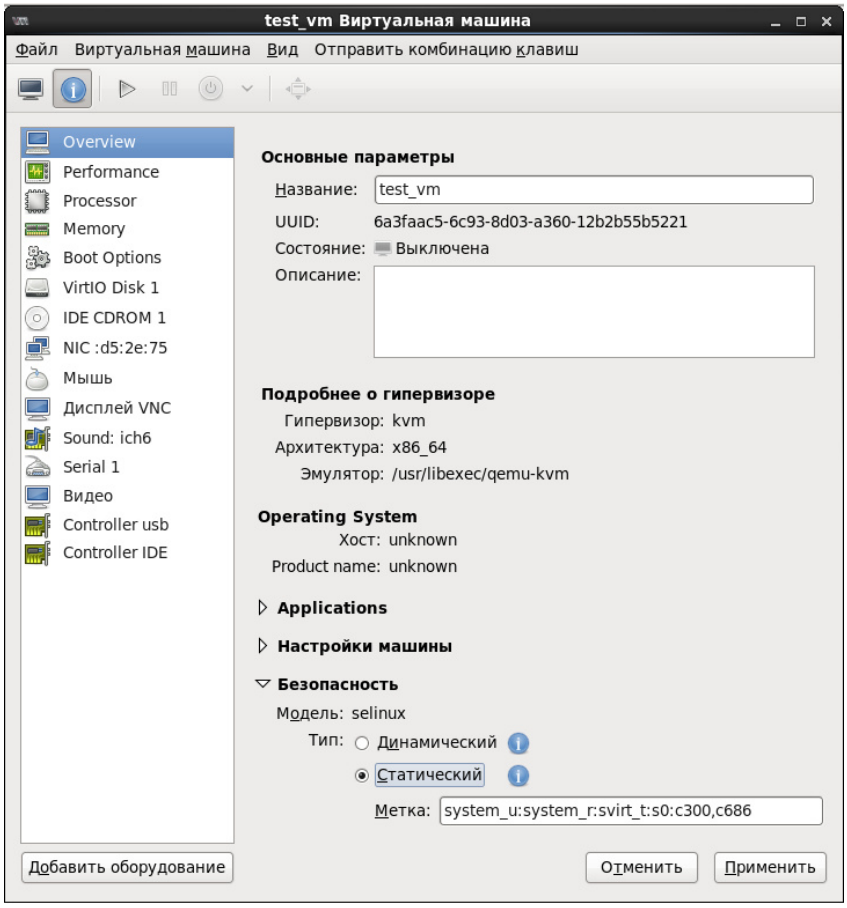


Рисунок 175 – Настройка виртуальной машины

8.9 Приложение "Конфигурация аутентификации"

Для настройки механизмов защиты идентификации и аутентификации пользователей в среде виртуализации предназначено приложение «Конфигурация аутентификации», которое запускается из меню системы, установленной на виртуальной машине «Система–>Администрирование–>Аутентификация» и доступно только в режиме администратора. Во вкладке «Идентификация и аутентификация» данного приложения нужно выбрать, как должна выполняться аутентификация пользователей. Соответствующее описание приведено в подразделе 3.2.

9 ФИЛЬТРАЦИЯ ПАКЕТОВ И МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ

9.1 Основные сведения

В МСВСфера 6.3 АРМ фильтрация сетевых пакетов реализована как на уровне ядра операционной системы, так и на уровне приложений пользователя.

Средства фильтрации пакетов и межсетевого экранирования предоставляют следующие возможности:

- преобразование сетевых адресов, скрытие подсети внутренней сети за одним или несколькими внешними IP-адресами с подменой источника во всех запросах;
- фильтрация приходящих от клиентов запросов определенного типа или протокола, на основании набора запрограммированных правил администратором;
- фильтрация пакетов через подсистему ядра Netfilter;
- фильтрация доступа к заведомо незащищенным службам;
- контроль доступа к узлам сети;
- ведение учёта использования доступа в Интернет отдельными узлами сети;
- регламентирование порядка доступа к сети;
- эффективное управление использованием ресурсов в сети.

Вышеперечисленные возможности фильтрации пакетов и межсетевого экранирования реализуются с помощью следующих программных компонент:

- приложение "Настройка Kickstart";
- подсистема Netfilter;
- приложение "Настройка межсетевого экрана";
- утилита iptables;
- утилита iptables-save;
- утилита iptables-restore;
- утилита ip6tables;
- утилита ebtables.

9.2 Приложение "Настройка Kickstart"

Программа "Настройка Kickstart", которая вызывается из меню "Приложения->Системные-> Kickstart", позволит создать настройки в файле kickstart для брандмауэра на вкладке "Настройка брандмауэра" (рис. 176), используя графический интерфейс.

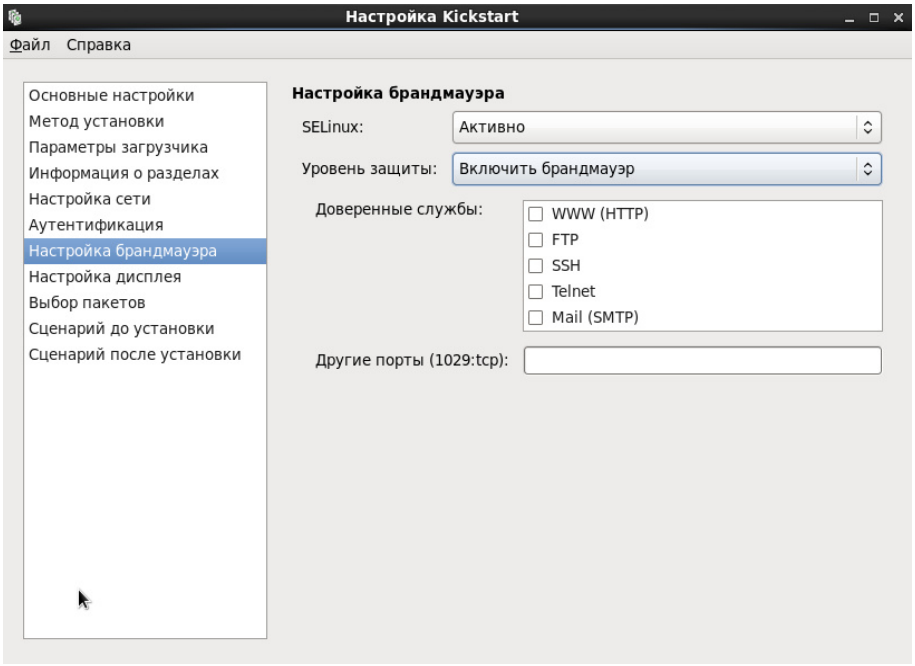


Рисунок 176 - Владка "Настройка брандмауэра"
приложения "Настройка Kickstart"

Параметр "SELinux". Хотя конфигурация SELinux не задаётся в этой программе, kickstart позволяет задать значения SELinux, как "Активно", "Режим предупреждений", "Отключено", подробнее о политике Selinux и ее режимах написано в разделах 4.5 и 4.6.

Параметр "Уровень защиты". Если выбран вариант "Отключить брандмауэр", система открывает полный доступ к любым активным службам и портам. Никакие подключения к системе не отклоняются и не запрещаются. Вариант "Включить брандмауэр" позволяет отклонять входящие подключения, кроме тех, что отвечают на исходящие запросы, как, например, ответы DNS или DHCP.

Параметр "Доверенные службы". В списке показываются устройства, с которых система будет принимать соединения. Например, если eth1 получает данные только от внутренних компьютеров, возможно, вы захотите разрешить подключения с этого устройства. Если служба

отмечена в списке "Доверенные службы", система принимает и обрабатывает подключения к этой службе.

Параметр "Другие порты". В текстовом поле можно перечислить дополнительные порты, которые следует открыть для удалённого доступа, в формате "port:protocol". Например, чтобы разрешить IMAP-доступ через брандмауэр, укажите "imap:tcp". Или укажите числовой номер порта, например, чтобы пропустить через брандмауэр UDP-пакеты в порт 1234, введите 1234:udp. Чтобы указать несколько портов, разделите их запятыми.

9.3 Подсистема Netfilter

Подсистемой ядра операционной системы, реализующей фильтрацию сетевых пакетов, является Netfilter. В системе Netfilter пакеты пропускаются через цепочки. Цепочка является упорядоченным списком правил. Каждое правило может содержать критерии и действие или переход. Когда пакет проходит через цепочку, система Netfilter по очереди проверяет, соответствует ли пакет всем критериям очередного правила, и если так, то выполняет действие. Если критериев в правиле нет, то действие выполняется для всех пакетов, проходящих через правило. Вариантов возможных критериев очень много. Стандартные действия доступные во всех цепочках: ACCEPT (пропустить), DROP (удалить), QUEUE (передать на анализ внешней программе), и RETURN (вернуть на анализ в предыдущую цепочку).

Существует пять типов стандартных цепочек, встроенных в систему:

- PREROUTING – для изначальной обработки входящих пакетов;
- INPUT – для входящих пакетов, адресованных непосредственно локальному процессу (клиенту или серверу);
- FORWARD – для входящих пакетов, перенаправленных на выход (перенаправляемые пакеты проходят сначала цепь PREROUTING, затем FORWARD и POSTROUTING);
- OUTPUT – для пакетов, генерируемых локальными процессами;
- POSTROUTING – для окончательной обработки исходящих пакетов.

С помощью утилиты iptables уровня пользователя можно создавать собственные цепочки.

Цепочки организованны в четыре таблицы:

- raw – просматривается до передачи пакета системе определения состояний. Используется редко, например, для маркировки пакетов, которые НЕ должны обрабатываться системой определения состояний. Для этого в правиле указывается действие NOTRACK. Содержит цепочки PREROUTING и OUTPUT;
- mangle – содержит правила модификации (обычно заголовка) IP-пакетов. Среди прочего, поддерживает действия TTL, TOS и MARK (для изменения полей TTL и TOS и для изменения маркеров пакета). Данную таблицу следует использовать с осторожностью. Содержит все пять стандартных цепочек;
- nat – просматривает только пакеты, создающие новое соединение согласно системе определения состояний. Поддерживает действия DNAT, SNAT, MASQUERADE, REDIRECT. Содержит цепочки PREROUTING, OUTPUT и POSTROUTING;
- filter – основная таблица используется по умолчанию, если название таблицы не указано. Содержит цепочки INPUT, FORWARD и OUTPUT.

Цепочки с одинаковым названием, но находящиеся в разных таблицах – совершенно независимые объекты. Например, raw PREROUTING и mangle PREROUTING обычно содержат разный набор правил. Пакеты сначала проходят через цепочку raw PREROUTING, а потом через mangle PREROUTING.

Важной частью Netfilter являются механизм определения состояний и система трассировки соединений (state machine, connection tracking), при помощи которых реализуется межсетевой экран на сеансовом уровне (stateful firewall). Система позволяет определить, к какому соединению или сеансу принадлежит пакет. Механизм определения состояний анализирует все пакеты кроме тех, которые были помечены NOTRACK в таблице raw.

В системе Netfilter, каждый пакет, проходящий через механизм определения состояний, может иметь одно из четырёх возможных состояний:

- NEW – пакет открывает новый сеанс. Пример – пакет TCP с флагом SYN;
- ESTABLISHED – пакет является частью уже существующего сеанса;
- RELATED – пакет открывает новый сеанс, связанный с уже открытым сеансом;
- INVALID – все прочие пакеты.

В состав системы Netfilter ядра ОС входят следующие модули:

- ip_tables – фаервол для протокола IPv4. Обеспечивает фильтрацию пакетов, модификацию их заголовков и трансляцию сетевых адресов;
- ip6_tables – фаервол для протокола IPv6. Обеспечивает фильтрацию пакетов и модификацию их заголовков;
- arp_tables – фаервол для протоколов ARP и RARP. Обеспечивает фильтрацию и модификацию пакетов;
- x_tables – бэкенд для ip_tables, ip6_tables и arp_tables. В этом модуле определены основные операции для работы с фаерволами «таблично-цепочечной» структуры и их компонентами;
- ebtables – Ethernet-фаервол (префикс eb от Ethernet Bridge). В отличие от трех перечисленных выше фаерволов, работающих с протоколами сетевого и более высоких уровней, ebtables работает на канальном уровне, выполняя фильтрацию и модификацию ethernet-кадров, проходящих через сетевые мосты, если таковые имеются на хосте.

Для взаимодействия с системой Netfilter предназначены следующие программы уровня пользователя:

- наборы утилит iptables и ip6tables;
- приложение system-config-firewall;
- утилита ebtables.

9.4 Утилита iptables

Утилита iptables предназначена для управления встроенным в ядро операционной системы фаерволом протокола IPv4. К ее задачам относятся:

- создание и удаление пользовательских цепочек;
- установка действий по умолчанию для базовых цепочек;
- добавление и удаление правил;
- установка и обнуление счетчиков пакетов и байт;
- вывод цепочек и правил, а также значений счетчиков;
- проверка корректности задания параметров, определяющих работу критериев и действий;
- вывод справки по использованию критериев и действий.

Рассмотрим интерфейс утилиты iptables. Чтобы запустить iptables вручную, нужно выполнить следующую команду:

/sbin/service iptables restart

Чтобы служба запускалась при загрузке системы, выполните команду:

/sbin/chkconfig --level 345 iptables on

При вызове утилиты в качестве параметра указывается команда, которую нужно выполнить. Обычно можно указать только одну команду, но есть исключения. Команду можно указать одной большой буквой или словом. Если при вызове любой команды не указано название таблицы, то команда выполняется в таблице filter. Программа имеет подробную справку, вызываемую командой man iptables.

1. Вывести правила (-L, --list) для указанной таблицы и цепочки:

iptables [-t таблица] -L [цепочка] [параметры]

Если цепочка не указана, то выводится список правил для каждой цепочки. Например, для вывода правил из таблицы nat необходимо выполнить команду:

iptables -t nat -n -L

2. Часто используются параметры "-n" (для избежания медленных запросов DNS) и "-v" (для вывода более подробной информации).

3. Команду "-L" можно использовать с "-Z" ("iptables -L -Z") для вывода значений счетчиков и одновременного их обнуления.

4. Удалить все правила из цепочки (-F, --flush):

iptables [-t таблица] -[F] [цепочка] [параметры]

Если цепочка не указана, то удаляются все цепочки из таблицы.

5. Обнулить все счетчики (-Z, --zero):

iptables [-t таблица] -Z [цепочка] [параметры]

Присваивает счетчикам числа пакетов и объема данных нулевые значения. Если цепочка не указана, то обнуление выполняется для всех цепочек.

6. Создать новую цепочку в указанной таблице с указанным именем (-N, --new-chain):

iptables [-t таблица] -N цепочка

Если в указанной таблице уже есть цепочка с указанным именем, то новая не создается.

7. Удалить цепочку, ранее созданную с помощью команды "-N" (-X, --delete-chain):

iptables [-t таблица] -X [цепочка]

Перед удалением цепочки необходимо удалить или заменить все правила, которые ссылаются на эту цепочку. Если цепочка не указана, то из таблицы будут удалены все цепочки, кроме стандартных (INPUT, OUTPUT, FORWARD, PREROUTING, POSTROUTING). Стандартные цепочки не удаляются.

8. Переименование цепочки (-E, --rename-chain):

iptables [-t таблица] -E цепочка новое_название

9. Установить политику для стандартной цепочки (-P, --policy):

iptables [-t таблица] -P цепочка действие [параметры]

Над пакетами, которые доходят до конца указанной цепочки, будет выполняться указанное действие. В качестве действия нельзя указывать название какой-либо цепочки. Устанавливать политику можно только на встроенных цепочках. Например, правила блокировки всех входящих и исходящих пакетов:

iptables -P INPUT DROP

iptables -P OUTPUT DROP

Чтобы все пересылаемые пакеты тоже были запрещены, нужно добавить правило:

iptables -P FORWARD DROP

Примечание: порядок правил имеет значение.

10. Добавить новое правило в конец указанной цепочки (-A, --append chain):

iptables [-t таблица] -A цепочка спецификация_правила [параметры]

Если в спецификации правила указано имя отправителя или получателя, которое одновременно соответствует нескольким адресам, то в конец цепочки добавляются правила для всех возможных комбинаций. Например, чтобы разрешить доступи к 80 порту брандмауэра, нужно выполнить команду:

iptables -A INPUT -p tcp -m tcp --sport 80 -j ACCEPT

iptables -A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT

Если ограничено количество маршрутизируемых в Интернете IP-адресов для организации и нужен доступ к Интернет-службам, не требующий назначения реальных IP-адресов каждому узлу локальной сети, то использование политики FORWARD позволит безопасно управлять маршрутизацией в локальной сети (исходящие запросы от локального узла к удаленной Интернет-службе).

Например, зададим правило для доступа к внутренней сети:

iptables -A FORWARD -i eth1 -j ACCEPT

iptables -A FORWARD -o eth1 -j ACCEPT

Чтобы маршрутизировать трафик к определённым компьютерам (например, к выделенному HTTP или FTP-серверу в демилитаризованной зоне) нужно использовать таблицу PREROUTING. Демилитаризованная зона (ДМЗ) - технология обеспечения защиты информационного периметра, при которой серверы, отвечающие на запросы из внешней сети, находятся в особом сегменте сети (который и называется ДМЗ) и ограничены в доступе к основным сегментам сети с помощью межсетевого экрана, с целью минимизировать ущерб при взломе одного из общедоступных сервисов, находящихся в зоне. Приведем пример, в котором создадим правило, где входящие HTTP-запросы будут маршрутизироваться к выделенному HTTP-серверу с IP-адресом 192.168.1.0 (ДМЗ, для которой будет выполняться преобразование адресов nat "один к одному", вне локальной сети 192.168.0.0/24 - доверительная внутренняя сеть), а NAT будет обращаться к таблице PREROUTING и передавать пакеты по назначению:

iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT \

--to-destination 192.168.1.0:80

В iptables включено отслеживание состояния соединений и классификация пакетов с точки зрения принадлежности к соединениям, что позволяет netfilter осуществлять полноценную stateful-фильтрацию трафика. Как и netfilter, система conntrack является частью ядра Linux. При помощи критерия conntrack можно классифицировать пакеты на основании их отношения к соединениям. В частности, состояние NEW позволяет выделять только пакеты, открывающие новые соединения, состояние ESTABLISHED — пакеты, принадлежащие к установленным соединениям, состоянию RELATED соответствуют пакеты, открывающие новые соединения, логически связанные с уже установленными, например, соединение данных в пассивном режиме FTP. Состояние INVALID означает, что принадлежность пакета к соединению установить не удалось. Например:

iptables -I INPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT

Заменив в предыдущем правиле "ESTABLISHED" на "ESTABLISHED,RELATED" и подгрузив соответствующие модули ядра, получим корректную фильтрацию протоколов, использующих связанные соединения - FTP, SIP, IRC, H.323 и других.

Изначально для определения состояния соединения использовался критерий state, то есть вместо "-m conntrack --ctstate ESTABLISHED,RELATED" использовалось "-m state --state ESTABLISHED,RELATED". Например, для пересылки пакетов, получаемых из внешнего соединения, используется отслеживание соединений:

iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ALLOW

11. Вставить новое правило в указанное место указанной цепочки (-I, --insert):

iptables [-t таблица] -I цепочка [номер_правила] спецификация_правила [параметры]

Правила нумеруются с 1, поэтому если указать номер 1 (или не указать вообще), то правило будет вставлено в начало цепочки.

12. Удалить правило (-D, --delete):

iptables [-t таблица] -D цепочка номер_правила [параметры]

iptables [-t таблица] -D цепочка спецификация_правила [параметры]

Правило можно указывать при помощи его номера в цепочке (нумерация начинается с 1) или его спецификации.

13. Заменить правило с указанным номером в указанной цепочке (-R, --replace):

iptables [-t таблица] -R цепочка номер_правила спецификация_правила [параметры]

Правила нумеруются с 1. Спецификация правила не может содержать имени отправителя или получателя, которое одновременно соответствует нескольким адресам.

Перечисленные ниже параметры используются при задании спецификации правил и указываются с командами модификации правил. Эти параметры ограничивают применение правил: если обрабатываемый пакет не соответствует указанным в спецификации критериям, то указанное в правиле действие на этот пакет не распространяется.

- [!] -p, --protocol протокол. Ограничение протокола. Основные значения: tcp, udp, icmp или all. Протокол также можно указать с помощью номера или названия, указанного в файле /etc/protocols. Знак «!» перед ключом изменяет критерий на противоположный. Значение «Любой протокол» можно указать с помощью слова all или числа 0. Если протокол не указан, то подразумевается «Любой протокол»;
- [!] -s, --src, --source адрес[/маска]. Ограничение отправителя. Адрес может быть IP-адресом (возможно с маской), именем хоста или доменным именем. Маска может быть в стандартном формате (например, 255.255.255.0) или же в виде числа, указывающего число единиц с «левой стороны» маски (например, 24). Знак «!» перед ключом изменяет критерий на противоположный. Настоятельно не рекомендуется

использовать имена, для разрешения которых требуется удаленный запрос, например, по системе DNS;

- [!] -d, --dst, --destination address[/mask]. Ограничение получателя. Синтаксис такой же, как у --src;
- [!] -i, --in-interface имя_интерфейса. Ограничение входящего сетевого интерфейса. Знак «!» перед адресом изменяет критерий на противоположный. Если указанное имя интерфейса заканчивается на «+», то критерию соответствуют все интерфейсы, чьи имена начинаются на указанное имя. Если параметр --in-interface не указан, то критерию соответствуют пакеты из любого сетевого интерфейса;
- -o, --out-interface [!] имя_интерфейса. Ограничение выходящего сетевого интерфейса. Синтаксис такой же, как и для --in-interface;
- [!] -f, --fragment. Ограничение по фрагментам: критерию соответствуют только фрагменты пакета, начиная со второго фрагмента. Знак «!» перед адресом меняет критерий на противоположный. У таких фрагментов, начиная со второго, нет заголовка с портами отправителя и получателя или с типом ICMP. Следовательно, такие фрагменты не соответствуют критериям, указывающим номера портов;
- -j, --jump действие_или_цепочка. Спецификация действий и переходов. Если указано название цепочки, ранее созданной командой -N, то пакеты, соответствующие критериям правила, переносятся в начало указанной цепочки (запрещено указывать название цепочки, в котором это правило находится). Если указано действие, то оно выполняется над пакетами, соответствующими критериям правила. Если в правиле нет параметров --jump и --goto, то правило не влияет на проверяемые пакеты, но счетчик правила продолжает работать;
- -g, --goto цепочка. --goto отличается от --jump поведением при действии RETURN. Действие RETURN переводит пакет в правило, следующее после того, которое вызвало предыдущий переход --jump. То есть, если пакет перешел из цепочки X в цепочку Y при помощи --jump, а потом в Z опять при помощи --jump, то действие RETURN из цепочки Z возвращает его в Y. Если же пакет перешел в Z при помощи --goto, то RETURN возвращает его в X;
- -c, --set-counters пакеты байты. Параметр позволяет при добавлении или изменении правил одновременно инициализировать счетчики числа пакетов и размера данных.

9.5 Утилита iptables-save

Утилита iptables-save предназначена для сохранения текущего набора правил в файл. Использование утилиты:

```
iptables-save [-M modprobe] [-c] [-t table]
```

Ключ "-M" позволяет указать путь до программы modprobe. По умолчанию путь берется из файла /proc/sys/kernel/modprobe.

Ключ "**-c**" (допустимо использовать более длинный вариант "--counters") заставляет iptables-save сохранить значения счетчиков байт и пакетов. Это делает возможным рестарт брандмауэра без потери счетчиков, которые могут использоваться для подсчета статистики. По умолчанию при запуске без ключа "**-c**", сохранение счетчиков не производится.

С помощью ключа "-t" (более длинный вариант "--table") можно указать имя таблицы для сохранения. Если ключ "-t" не задан, то сохраняются все таблицы.

9.6 Утилита iptables-restore

Утилита iptables-restore используется для восстановления (загрузки) набора правил, который ранее был сохранен утилитой iptables-save. Набор правил утилита получает со стандартного ввода и не может загружать его из файла напрямую. Команда имеет следующий синтаксис:

iptables-restore [-c] [-n]

Ключ "**-c**" (более длинный вариант "--counters") заставляет восстанавливать значения счетчиков.

Указание ключа "**-**n" (более длинный вариант "--noflush") сообщает iptables-restore о том, что правила должны быть добавлены к имеющимся. По умолчанию утилита iptables-restore (без ключа "-n") очистит содержимое таблиц и цепочек перед загрузкой нового набора правил.

9.7 Утилита ip6tables

Утилита ip6tables предназначена для управления встроенным в ядро операционной системы фаерволом протокола IPv6. Интерфейс утилиты аналогичен интерфейсу утилиты iptables.

Утилиты ip6tables-save, ip6tables-restore выполняют те же задачи, что и утилиты iptables-save, ip6tables-restore, но применительно к IPv6.

9.8 Утилита ebtables

Утилита ebtables – средство для фильтрации и трансляции адресов пакетов на сетевых интерфейсах и программных мостах Linux. ebtables похоже на iptables, но отличается тем, что работает преимущественно не на третьем, а на втором уровне сетевого стека. Как и iptables, ebtables позволяет не только фильтровать пакеты, но и изменять их адреса, то есть выполнять трансляцию адресов на канальном уровне.

Программа поддерживает три таблицы ядра операционной системы с цепочками правил для кадров Ethernet. Таблицы ядра используются для распределения функциональности по нескольким наборам правил – цепочкам. Каждая цепочка представляет собой набор упорядоченных правил соответствия для кадров Ethernet. Если данный кадр соответствует правилу, для этого кадра применяется заданная правилом операция (target). Если же кадр не соответствует спецификации данного правила, этот кадр передается следующему правилу цепочки и т. д. Пользователь может создавать свои цепочки, которые могут служить в качестве операций для встроенных и пользовательских цепочек.

Как было отмечено, программа поддерживает три таблицы для кадров Ethernet: filter**,** nat и broute. По умолчанию все операции (правила) ebtables относятся к таблице filter.

Используемая по умолчанию таблица filter содержит три встроенных цепочки: INPUT (для кадров, адресованных данному хосту), OUTPUT (для кадров, сгенерированных данным хостом) и FORWARD (для пересылаемых мостом кадров).

Таблица nat служит для изменения MAC-адресов и содержит три встроенных цепочки: PREROUTING (изменение кадров на входе), OUTPUT (изменение локально сгенерированных кадров до передачи их мосту) и POSTROUTING (изменение кадров на выходе).

Таблица broute служит для выполнения функций моста-маршрутизатора (brouter) и включает одну цепочку – BROUTING. Операции DROP и ACCEPT для таблицы broute имеют отличный от общепринятого смысл. DROP означает, что кадр будет маршрутизироваться, а

ACCEPT говорит об использовании для кадра функций моста. Цепочка BROUTING используется на самых ранних этапах обработки пакетов. В эту цепочку передаются только пакеты, принимаемые через интерфейсы моста, которые находятся в состоянии forwarding (пересылка пакетов). Обычно для пересылки кадров используются функции моста, но можно поступить иначе. Для этого очень удобна операция redirect**.**

Для указания таблицы используется опция `-t <имя_таблицы>`.

Основные ключи утилиты ebtables:

- `-A, --append`. Добавляет правило в конец указанной цепочки;
- `-D, --delete`. Удаляет заданное правило из указанной цепочки. Удаляемое правило можно указать по его номеру или использовать в команде спецификацию условий и действие, в точности соответствующие правилу, которое нужно удалить. При удалении правил по номеру можно удалить сразу несколько правил, задав диапазон номеров в форме start_nr[:end_nr]. При удалении правил по номерам допускается использовать отрицательные значения номеров, смысл которых разъясняется в описании команды `-I`;
- `-I, --insert`. Вставляет правило в указанную номером строку списка. Если в цепочке имеется N правил, в качестве параметра команды I можно использовать значения от -N до N+1. Для случая положительных значений i, позиции с номером i-N-1 и i. Нулевое значение задает вставку правила вслед за последним из имеющихся в таблице правил как по команде `-A`;
- `-P, --policy`. Задает политику для данной цепочки. В качестве политики могут использоваться операции ACCEPT**,** DROP **и** RETURN;
- `-F, --flush`. Удаляет все правила из указанной цепочки. Если цепочка не указана, удаляются правила из всех цепочек. Удаление из цепочки всех правил не меняет выбранной для этой цепочки политики;
- `-Z, --zero`. Устанавливает нулевые значения счетчиков пакетов и байтов для указанной цепочки. Команду **`-z`** можно использовать вместе с командой просмотра списка правил `-L`. При таком использовании команд на экран выводится список правил с текущими значениями счетчиков, после чего все счетчики сбрасываются;
- `-L, --list`. Выводит на экран список правил указанной цепочки. Команда `-L` поддерживает ряд опций;

- `-N, --new-chain`. Создает новую пользовательскую цепочку с заданным именем. Имя цепочки может содержать до 31 символа, число пользовательских цепочек не ограничено;
- `-X, --delete-chain`. Удаляет указанную пользовательскую цепочку. Удалить можно только те цепочки, которые не используются в качестве операции в какой-либо из остающихся цепочек. Если команда вводится без имени цепочки, ebtables будет удалять все неиспользуемые пользовательские цепочки;
- `-E, --rename-chain`. Переименовывает указанную цепочку. В отличие от iptables программа ebtables позволяет менять имена не только у пользовательских, но и у встроенных цепочек. Например, можно переименовать в PREBRIDGING цепочку PREROUTING, с помощью команды -E `PREROUTING`. Переименование цепочек не оказывает никакого влияния на работу ebtables**;**
- `--init-table`. Сбрасывает все цепочки таблицы в исходное состояние;
- `--atomic-init`. Копирует инициализационные данные для таблицы в файл. Эту команду можно использовать для сохранения инициализационной таблицы с целью последующего добавления в нее команд. Файл задается с помощью опции **--**`atomic-file` или указывается в переменной окружения EBTABLES_ATOMIC_FILE**;**
- `--atomic-save`. Копирует текущую информацию из таблицы ядра в файл. Эту команду можно использовать для сохранения текущей таблицы с целью последующего добавления в нее команд. Файл задается с помощью опции `--atomic-file` или указывается в переменной окружения EBTABLES_ATOMIC_FILE**;**
- `--atomic-commit`. Заменяет таблицу ядра данными из указанного файла. Эта команда может быть весьма полезна при настройке правил, когда пользователь может загрузить таблицы из сохраненного ранее файла и вносить в нее пошаговые изменения. Загружаемые таблицы должны быть записаны в файл с помощью команды `--atomic-init` или `--atomic-save`. Файл, с которым работает данная команда, задается с помощью опции `--atomic-file` или указывается в переменной окружения EBTABLES_ATOMIC_FILE**;**
- `--atomic-file -Z`. Команда `--atomic-file` может использоваться вместе с командой `-Z` для обнуления значений счетчиков при записи в файл. Обнуление счетчиков возможно и с помощью переменной окружения EBTABLES_ATOMIC_FILE.

9.9 Приложение "Настройка межсетевого экрана"

Графическое приложение "Настройка межсетевого экрана" также как и iptables позволяет управлять фаерволом, встроенным в ядро операционной системы, но на более высоком и удобном для пользователя уровне. Вызывается из меню «Система–>Администрирование–>Межсетевой экран» или вводом команды в консоли "system-config-firewall".

Настроить межсетевой экран можно, используя "Мастер настройки межсетевого экрана" (запускается кнопкой "Мастер" на панели быстрого доступа приложения "Настройка межсетевого экрана"), или непосредственно изменяя параметры на вкладках приложения.

"Мастер настройки межсетевого экрана" предлагает ответить на заданные им вопросы в режиме диалога (рис. 177). Созданные настройки можно будет позже изменить в меню "Параметры" главного окна приложения. Для перехода к следующему шагу нужно нажать кнопку "Вперед".

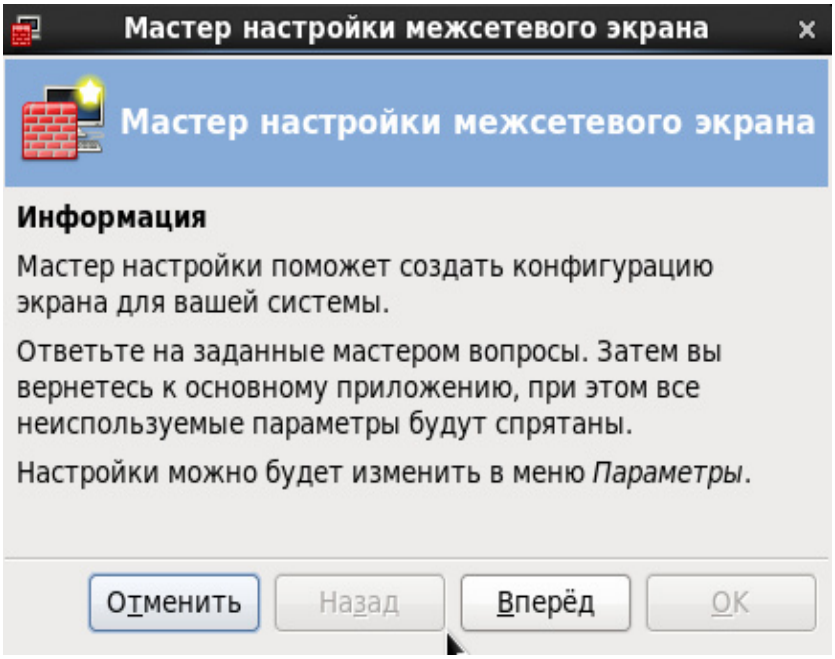


Рисунок 177 - Окно приветствия приложения "Мастер настройки межсетевого экрана"

В окне, приведенном на рис. 178, нужно задать тип системы - с или без сетевого доступа. Если будет выбран тип - "Система без сетевого доступа" - межсетевой экран будет отключен. После выбора нужно нажать кнопку "Вперед".

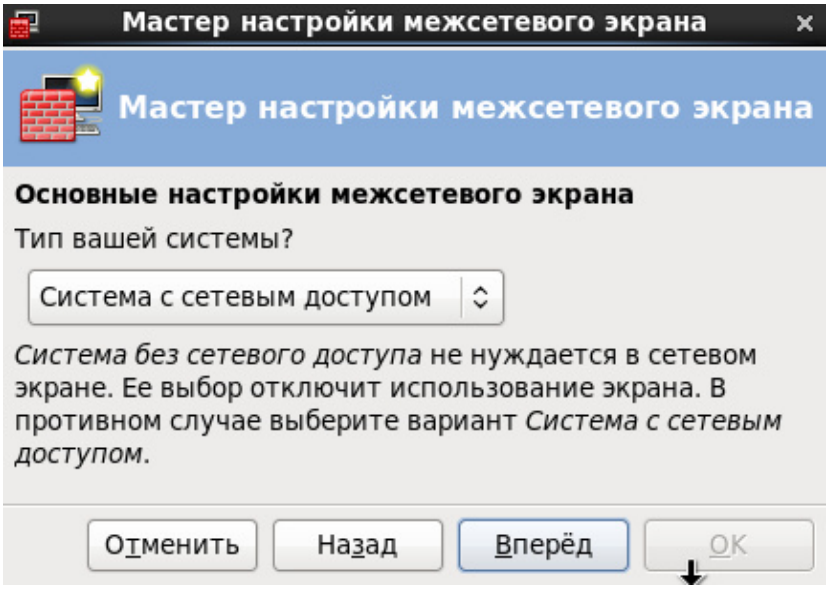


Рисунок 178 - Окно выбора типа системы

Далее нужно задать уровень работы пользователя с межсетевым экраном - "Эксперт" или "Начинающий" (рис. 179). Если вы выберете уровень "Начинающий", то в окне настроек межсетевого экрана в последующем останется только вкладка "Доверенные службы", а для добавления собственных правил и более глубокой настройки межсетевого экрана нужно выбрать уровень "Эксперт". После выбора нужно нажать кнопку "Вперед".

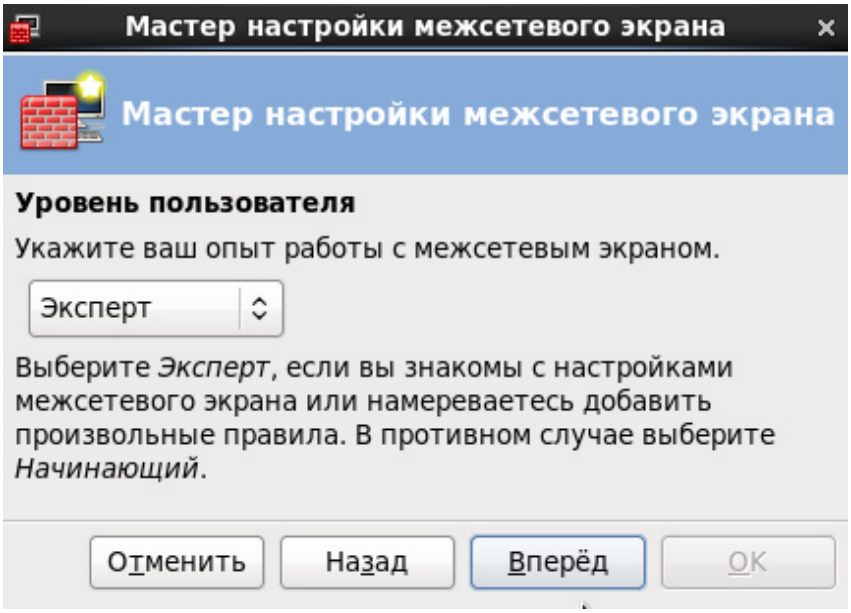


Рисунок 179 - Окно выбора уровня работы с межсетевым экраном пользователя

В окне, приведенном на рис. 180, нужно определиться с конфигурацией, здесь можно оставить текущую конфигурацию или загрузить конфигурацию для рабочей станции или сервера, сняв галочку с пункта "Оставить конфигурацию" и выбрав соответствующее значение поля. После выбора нужно нажать кнопку "Вперед".

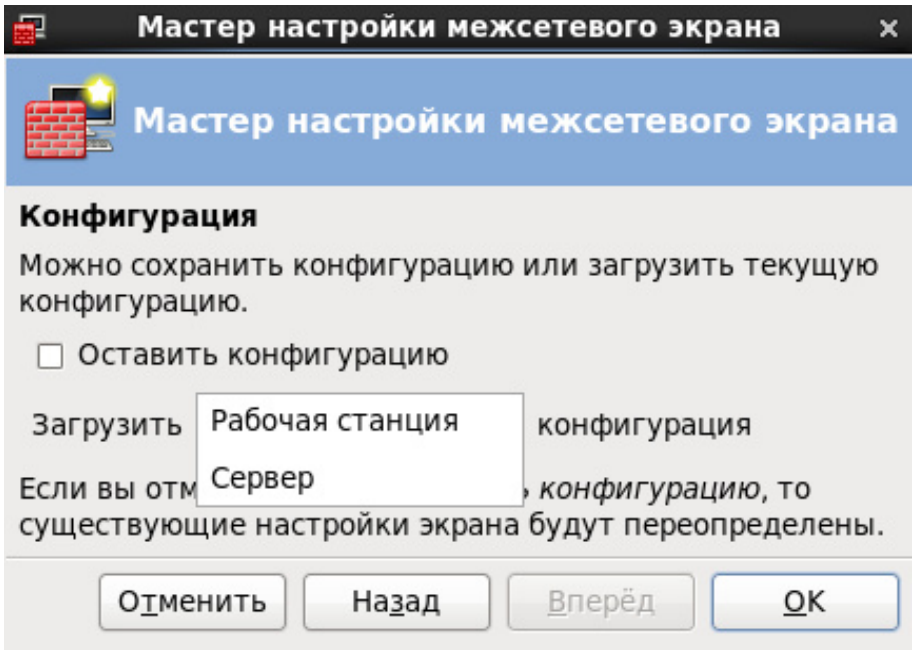


Рисунок 180 - Окно выбора конфигурации межсетевого экрана

При уровне "Эксперт", типе "Система с сетевым доступом" и конфигурацией "Рабочая станция" на вкладке "Доверенные службы" подключатся следующие службы, которые будут доступны из любых сетей и узлов:

- IPsec (Internet Protocol Security) - обеспечивает защиту при сетевой передаче напрямую к IP и предоставляет методы шифрования данных и аутентификации целевого узла или сети, если вы намереваетесь использовать сервер vpnc или freeS/WAN, не отключайте данную опцию;
- mDNS (Multicast DNS) - предоставляет возможность использования интерфейсов программирования DNS, форматов пакетов и операционной семантики в небольших сетях без стандартного DNS-сервера, если вы намереваетесь работать с Avahi, не отключайте данную опцию;
- Клиент Samba - эта опция позволяет получить доступ и работать в сети с Windows с общим доступом к файлам и принтерам, для того, чтобы данная настройка вступила в силу, необходимо установить пакет samba-client;

- Клиент сетевой печати (IPP) - протокол печати, который используется для осуществления распределенной печати, IPP (через tcp) дает возможность получить информацию о принтере (например, его возможности и состояние), а также может управлять заданиями печати, если вы намереваетесь настроить сетевой принтер для печати через cups, не отключайте эту опцию.

При уровне "Эксперт", типе "Система с сетевым доступом" и конфигурацией "Сервер" на вкладке "Доверенные службы" подключатся следующая служба, которая будет доступна из любых сетей и узлов:

- SSH (Secure Shell) - протокол для подключения и выполнения команд на удаленных системах, обеспечивает безопасное шифрованное взаимодействие. Если вы планируете подключаться к машине удаленно по SSH через защищенный экраном интерфейс, то понадобится установить пакет openssh-server, для того, чтобы обеспечить работу SSH-сервера на вашем компьютере.

Настройка параметров брандмауэра.

На панели быстрого доступа находятся кнопки управления настройками межсетевого экрана. Кнопки "Включить" и "Выключить" регулируют непосредственную работу межсетевого экрана. Кнопка "Применить" позволяет принять измененные настройки межсетевого экрана, заданные во время работы с приложением. Кнопка "Перезагрузить" позволяет перезагрузить текущую конфигурацию. Пункт меню "Параметры" позволяет задать параметры, настраиваемые в "Мастере настройки межсетевого экрана".

В списке «Доверенные службы» (рис. 181) показаны те службы, которые будут доступны из любых сетей и узлов. Для каждой службы есть подсказка (нужно подвести указатель мыши к службе) о ее настройке и назначении. Например, если вам требуется разрешить удаленным узлам подключаться непосредственно к вашей системе для доставки почты, то подключите опцию "Почта SMTP", межсетевой экран разрешит входящую доставку SMTP почты. Вам не нужно включать эту опцию, если вы получаете почту с сервера провайдера (ISP) по протоколам POP3 или IMAP, или если вы используете утилиты типа fetchmail. Обратите внимание, что некорректно настроенный SMTP сервер может разрешить удаленныма машинам использовать ваш сервер для рассылки спама.

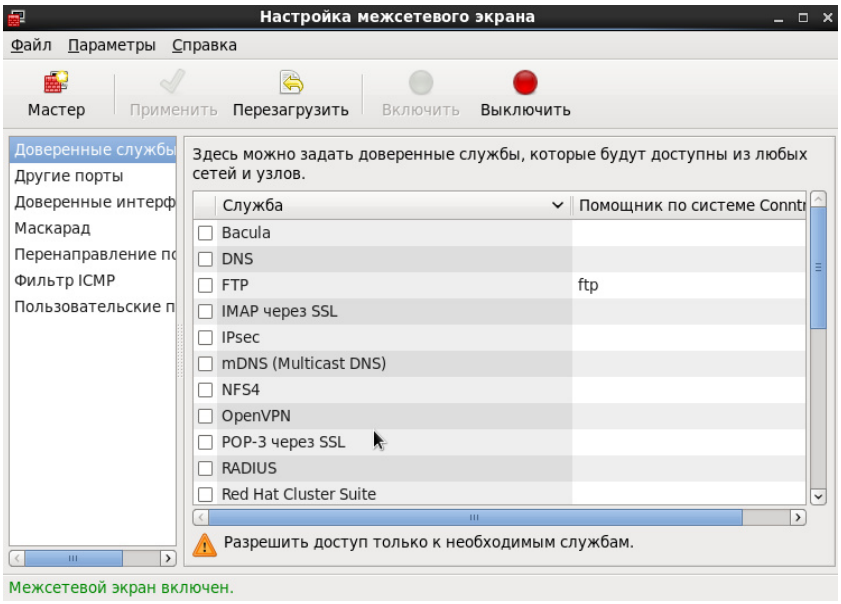


Рисунок 181 – Вкладка "Доверенные службы"

В списке «Другие порты» можно перечислить дополнительные порты, которые следует открыть для удаленного доступа.

Можно добавить, изменить и удалить порты соответствующими кнопками. Используйте формат `порт:протокол` при добавлении портов (рис. 182). Например, чтобы разрешить IMAP-доступ через экран, необходимо указать `imap:tcp`. Также можно явно задать числовой номер порта. Например, чтобы пропустить UDP-пакеты через 1234, необходимо задать `1234:udp`. При указании нескольких портов они разделяются запятыми.

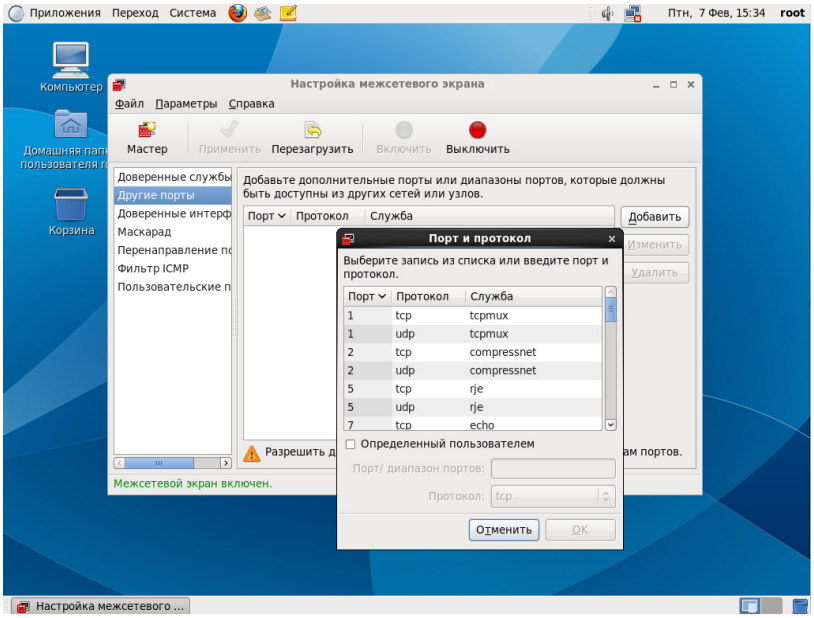


Рисунок 182 - Добавление порта и протокола

В списке «Доверенные интерфейсы» (рис. 183) показаны устройства, которые получат полный доступ к системе. Например, если eth1 получает данные только от внутренних компьютеров, возможно, вы захотите разрешить подключения с этого устройства.

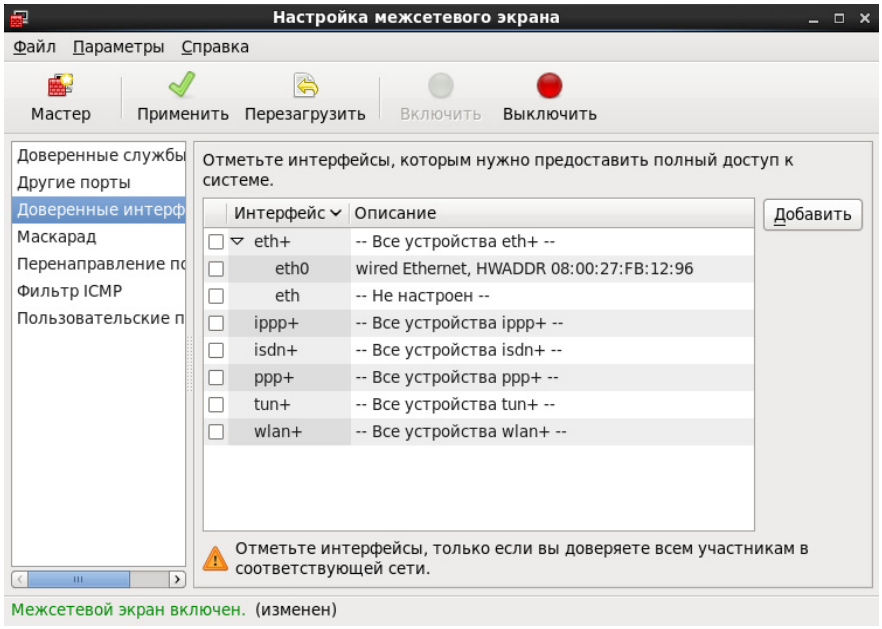


Рисунок 183 - Вкладка "Доверенные интерфейсы"

Вкладка «Маскарад» (рис. 184) предоставляет возможность настроить узел или маршрутизатор, подключающий локальную сеть к Интернету. Локальная сеть при этом не будет видна извне, будет доступен только один адрес. Кнопка "Добавить" позволяет добавлять устройство.

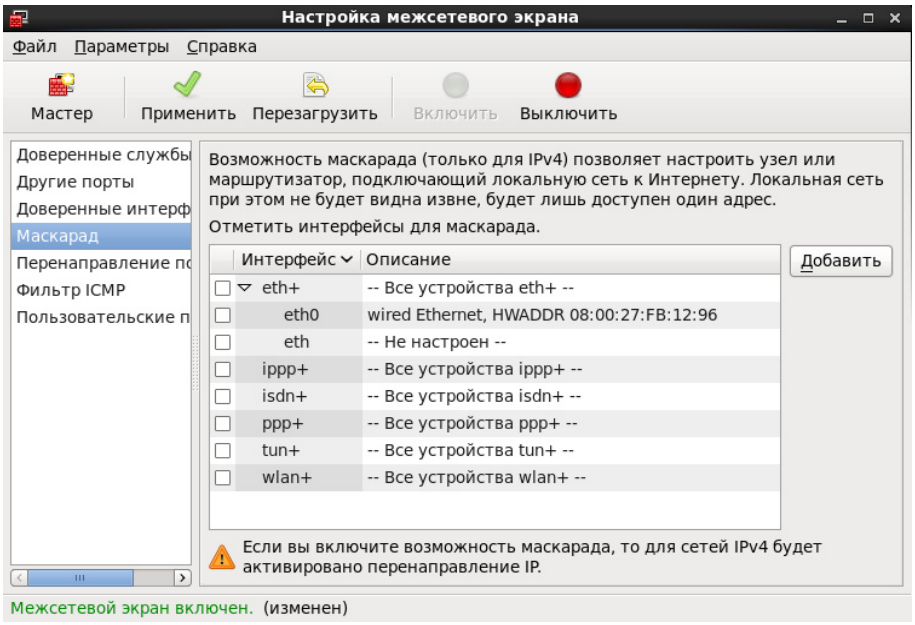


Рисунок 184 - Вкладка "Маскарад"

Вкладка «Перенаправление портов» позволяет добавить записи для перенаправления портов либо с одного порта другому в локальной системе, либо из локальной системы другой системе (например, при маскараде интерфейса). На рис. 185 видно, что для добавления портов нужно указать параметры источника и цели, а именно выбрать интерфейс, протокол и порт в одноименных полях, задать для целевого порта (порт, отличный от источника) в удаленной системе параметры: "Локальное перенаправление", "Направить другому порту" и задать "Адрес IP" и "Порт".

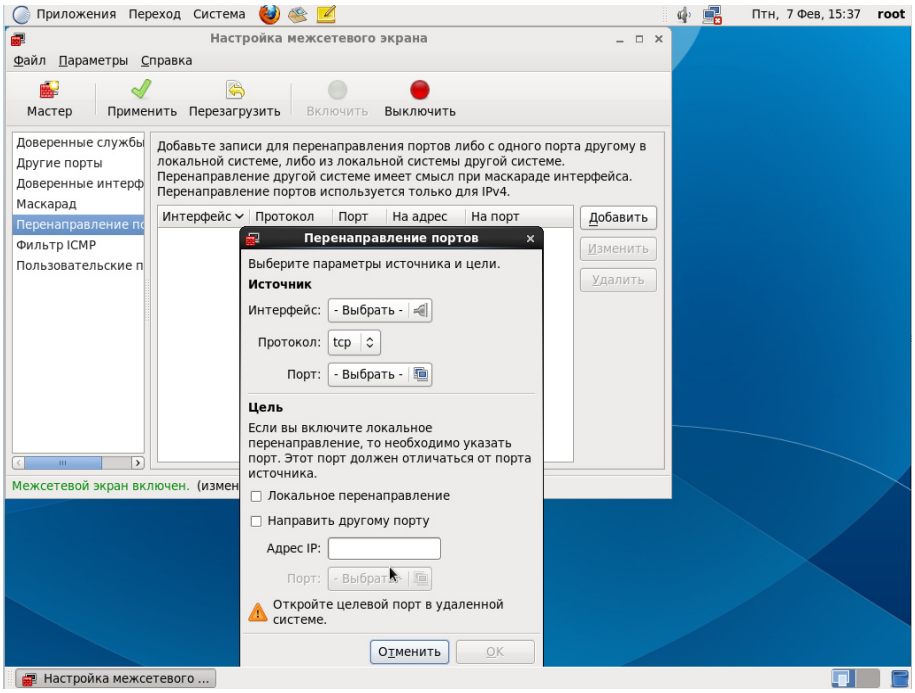


Рисунок 185 - Перенаправление портов

Приложение предоставляет возможность фильтрации протокола ICMP. В списке «Фильтр ICMP» можно указать типы сообщений ICMP, которым следует отказать в прохождении через межсетевой экран (рис. 186).

Типы ICMP:

- Время превышено — это сообщение об ошибке генерируется в случае превышения значения «time-to-live» пакета или повторно собранного фрагментированного пакета;
- Замедление источника — это сообщение об ошибке говорит узлу уменьшить скорость отправки пакетов;
- Запрос маршрутизатора — это сообщение используется узлом, соответствующим многоадресной ссылке, для запроса объявления маршрутизатора;

- Объявление маршрутизатора — это сообщение используется маршрутизаторами для периодического объявления IP-адреса широковещательного интерфейса;
- Перенаправление — это сообщение об ошибке информирует шлюз о том, что надо направить пакет по другому маршруту;
- Проблема принтера - это сообщение об ошибке генерируется, если неверен заголовок IP, например, отсутствует параметр или его длина не верна;
- Цель недоступна - это сообщение генерируется узлом или шлюзом, если цель недоступна;
- Эхо-запрос (пинг) - это сообщение будет использоваться для проверки возможности доступа к узлу с помощью утилиты ping;
- Эхо-ответ (pong) — это ответ на эхо-запрос.

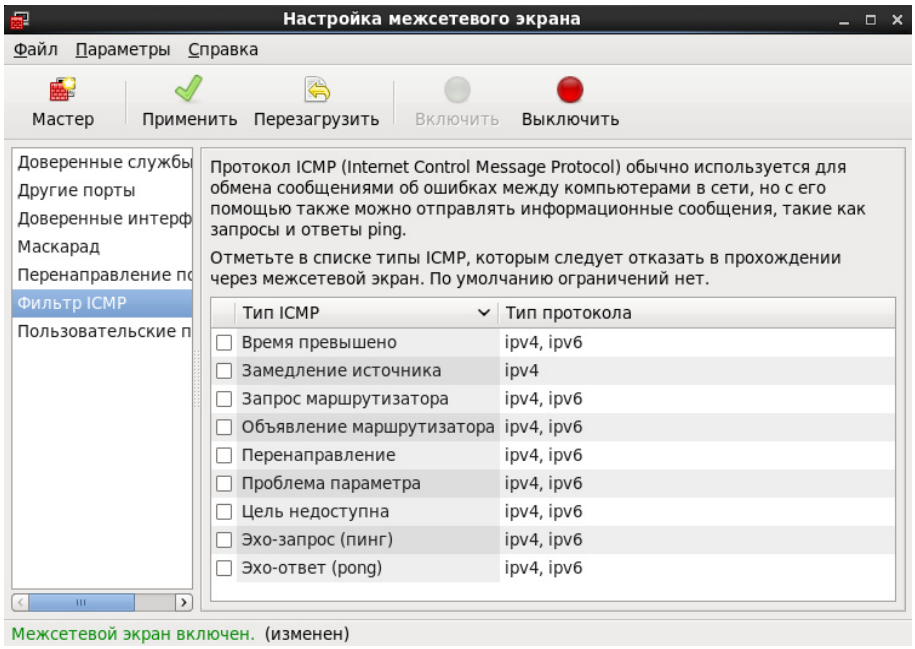


Рисунок 186 - Вкладка "Фильтр ICMP"

Также приложение позволяет задавать пользовательские правила межсетевого экрана на вкладке "Пользовательские правила". Для добавления правил используются файлы в формате iptables-save. Нажав кнопку "Добавить" появится диалоговое окно (рис. 187), в котором нужно указать тип протокола, таблицу экрана, путь к файлу и утвердить изменения кнопкой "ОК". О таблицах экрана подробнее в подразделе 9.3.

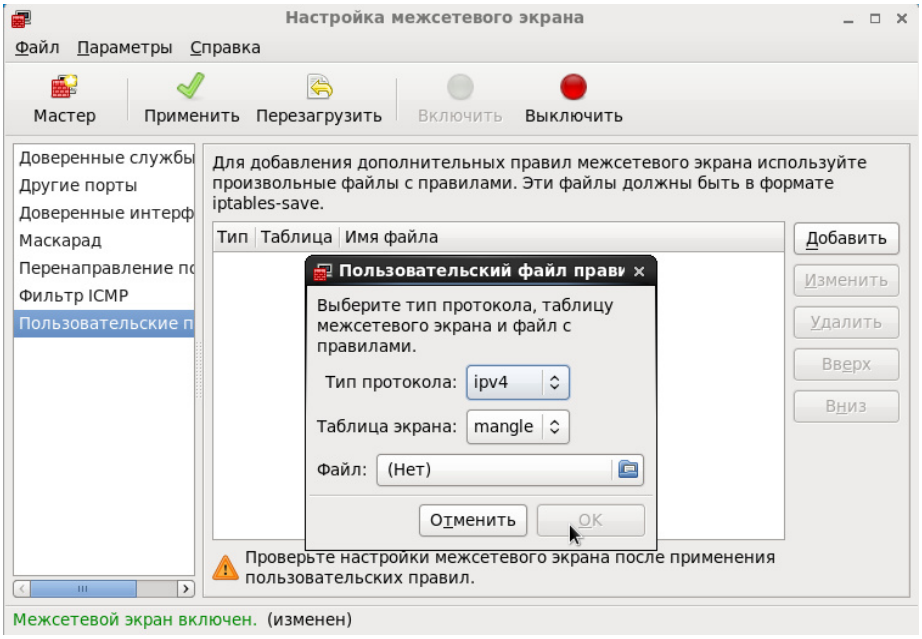


Рисунок 187 - Вкладка "Пользовательские правила"

Изм.	Лист	№ докум	Подп	Дата

10 ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ

10.1 Основные сведения

С целью обеспечения целостности программной среды установка и обновление операционной системы должны проводиться только с помощью доверенных инсталляционных дистрибутивов (компакт-дисков, удаленных репозиториев, внешних накопителей и т.п.). В процессе эксплуатации рекомендуется периодически осуществлять проверку целостности исполняемых файлов.

В МСВСфера 6.3 АРМ имеются средства контроля целостности устанавливаемых пакетов посредством проверки их подписи с помощью специального (проверочного) ключа, идущего в комплекте поставки вместе с дистрибутивом и устанавливаемого автоматически, а также средства контроля целостности исполняемых файлов в процессе эксплуатации системы.

10.2 Контроль целостности при установке и обновлении системы.

В ходе инсталляции и обновления системы проверка подписей устанавливаемых пакетов осуществляется менеджером пакетов и включается следующими настройками в конфигурационном файле:

- параметру gpgcheck присваивается значение, равное 1;
- параметру gpgkey присваивается путь к проверочному gpg-ключу.

По умолчанию, менеджер пакетов настроен на установку и обновление с компакт-диска:

```
[InstallCD]
name=MSVSphere 6.3 ARM
baseurl=file:///media/MSVSphere_6.3_ARM
enabled=0
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-MSVSphere
```

[UpdatesCD]

name=Updates from CD

baseurl=file:///media/MSVSphere_6.3_ARM_Updates/Updates

enabled=0

gpgcheck=1

gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-MSVSphere

Для разрешения операций установки и обновления пакетов необходимо установить параметру enabled значение, равное 1:

enabled=1

При необходимости обновления из удаленного репозитория следует указать адрес репозитория:

[fromhttp]

name=Updates from http

baseurl=http://<адрес репозитория>

enabled=1

gpgcheck=1

gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-MSVSphere

После обновления системы целостность пакетов можно проверять с помощью команды в консоли

md5sum <имя_файла.расширение>, как показано на рис. 188.

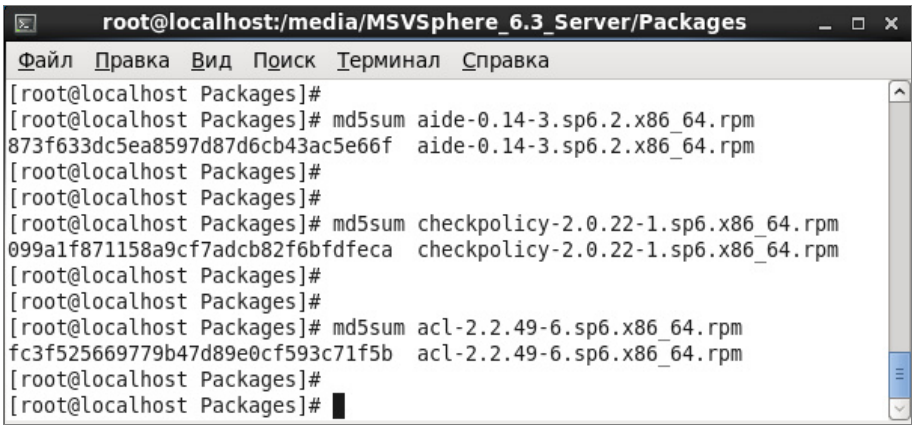


Рисунок 188 – Проверка целостности пакетов

10.3 Контроль целостности в процессе эксплуатации системы.

В качестве инструментального средства контроля целостности системы в процессе эксплуатации можно использовать утилиту AIDE.

Утилиту AIDE рекомендуется установить при инсталляции системы, для чего в ручном режиме надо выбрать для установки все программы, реализующие средства безопасности. Если утилита AIDE не была установлена при инсталляции системы, выполните следующие действия с правами администратора:

1. Задайте в конфигурационном файле значение параметра enabled=1.

name=MSVSphere 6.3 ARM

baseurl=file:///media/MSVSphere_6.3_ARM

enabled=1

gpgcheck=1

gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-MSVSphere

2. Вставьте в устройство чтения оптических дисков инсталляционный компакт-диск и дождитесь его автоматического монтирования.

3. Выполните команду в консоли

yum install aide

Файл конфигурации утилиты AIDE находится в /etc/aide.conf.

Указать каталог, в котором будет храниться база контрольных сумм, можно в строке:

@@define DBDIR /var/lib/aide

Задать в каком файле будет храниться информация о контрольных суммах, времени модификации защищаемых файлов и каталогов, можно в следующей строке:

database=file:@@{DBDIR}/aide.db.gz

Предположим, что в файл aide.db.new.gz будет помещена информация о сгенерированных контрольных суммах файлов при запуске процесса инициализации aide –init, для этого укажем его в следующей строке:

database_out=file:@@{DBDIR}/aide.db.new.gz

Для указания работы со сжатым форматом файлов, укажем флаг YES в строке:

gzip_dbout=yes

Задать уровень детализации можно в строке:

verbose=5

Необходимо также указать файл, в который будет сохраняться информация о ходе проверки:

report_url=file:/var/log/aide.log

Для вывода информации на экран, нужно задать поток stdout, как в следующей строке:

report_url=stdout

Проверкой целостности можно управлять, указывая другие параметры для конфигурационного файла aide.conf:

#p: разрешения на файл

#i: дескриптор inode

#n: количество ссылок

#u: пользователь

#g: группа

#s: размер

#b: количество блоков

#m: mtime - время последней модификации

#a: atime - время последнего доступа

#c: ctime - время последнего изменения атрибутов файла

#S: check for growing size

#acl: Access Control Lists

#selinux SELinux security context

#xattrs: Extended file attributes

Алгоритмы хеширования

#md5: md5 checksum

#sha1: sha1 checksum

#sha256: sha256 checksum

#sha512: sha512 checksum

#rmd160: rmd160 checksum

#tiger: tiger checksum

#haval: haval checksum (MHASH only)

#gost: gost checksum (MHASH only)

#crc32: crc32 checksum (MHASH only)

#whirlpool: whirlpool checksum (MHASH only)

Группы разрешений

#R: p+i+n+u+g+s+m+c+acl+selinux+xattrs+md5

#L: p+i+n+u+g+acl+selinux+xattrs

#E: Empty group

#>: Growing logfile p+u+g+i+n+S+acl+selinux+xattrs

В файле можно создать шаблон, указав его имя, знак равно и перечень параметров, разделенных знаком "+", как например:

NORMAL = R+b+sha1

Проверить каталог можно, указав путь к нему и имя шаблона через пробел. Например, для проверки каталога boot по шаблону NORMAL нужно указать следующее:

/boot NORMAL

Можно также указать, какие проверки проводить в каталоге с помощью предопределенных проверок:

/etc p+i+u+g

Можно исключить отдельные файлы из области проверки:

!/etc/mtab

Например, есть множество файлов, для которых происходят периодические изменения (логи, файлы-флаги, файлы-семафоры, файлы с идентификаторами процессов и т.д.). Проверка контрольных сумм таких файлов не имеет смысла. Поэтому при обнаружении, их следует вручную удалить из конфигурационного файла aide.conf. Автоматически из этого списка удаляются:

/etc/adjtime

/etc/hosts

/etc/mtab

/var/log/*

/var/run/*

После уточнения конфигурации необходимо сгенерировать базу контрольных сумм файлов, для этого нужно задать команду инициализации

aide --init, как показано на рис. 189.

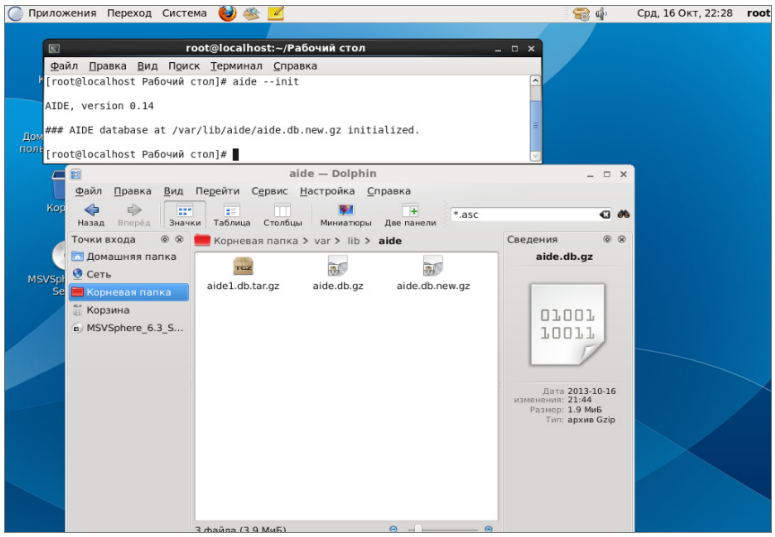


Рисунок 189 - Инициализация AIDE

В результате получим сгенерированную базу контрольных сумм /var/lib/aide/aide.db.new.gz. Пример содержимого базы представлен на рис. 190.

Рисунок 190 - База контрольных сумм aide.db.new.gz

Затем сгенерированную базу контрольных сумм с помощью команды в режиме администратора

mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz

перемещаем в ее стандартное положение /var/lib/aide/aide.db.gz, как на рис. 191.

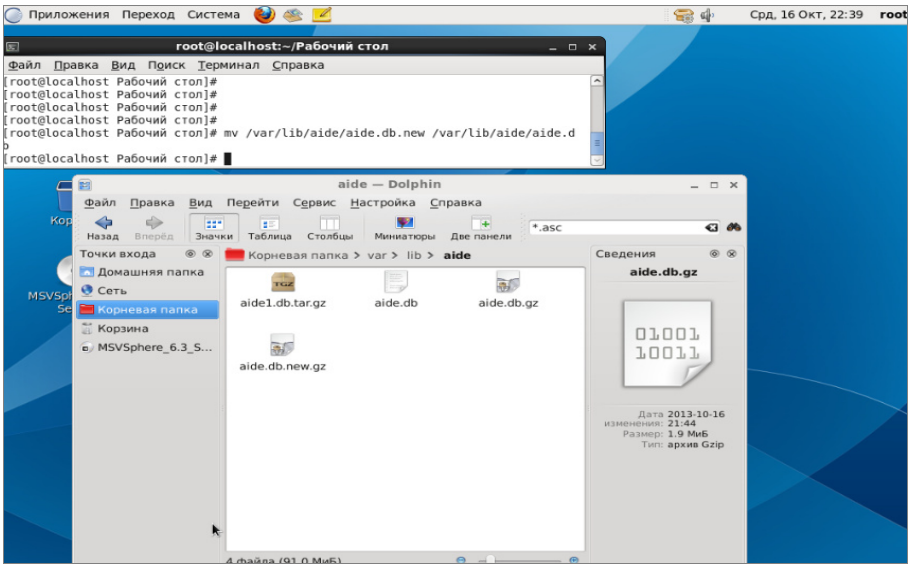


Рисунок 191 - Перемещение базы данных AIDE

Для последующей проверки необходимо выполнить команду aide --check. Отчет о результатах проверки будет выведен в консоль (рис. 192). Проверка считается успешной, если отчет не содержит информации об измененных и удаленных файлах. В противном случае можно сделать вывод о нарушении целостности системы.

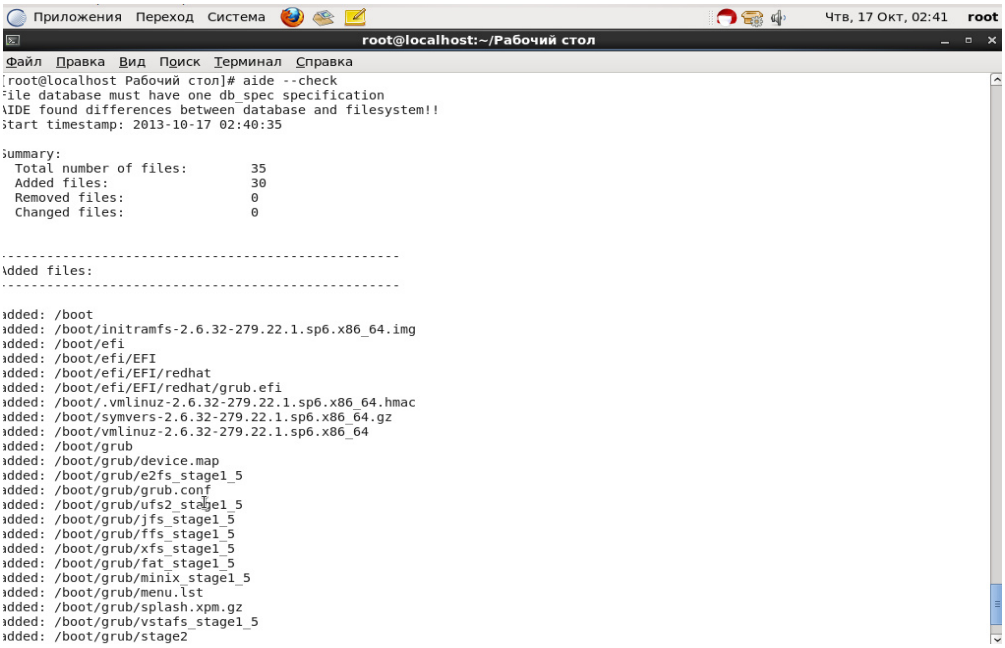


Рисунок 192 - Выполнение aide --check

Информацию о контрольных суммах, времени модификации контролируемых файлов и каталогов, можно будет увидеть в aide.db.gz (рис. 193).

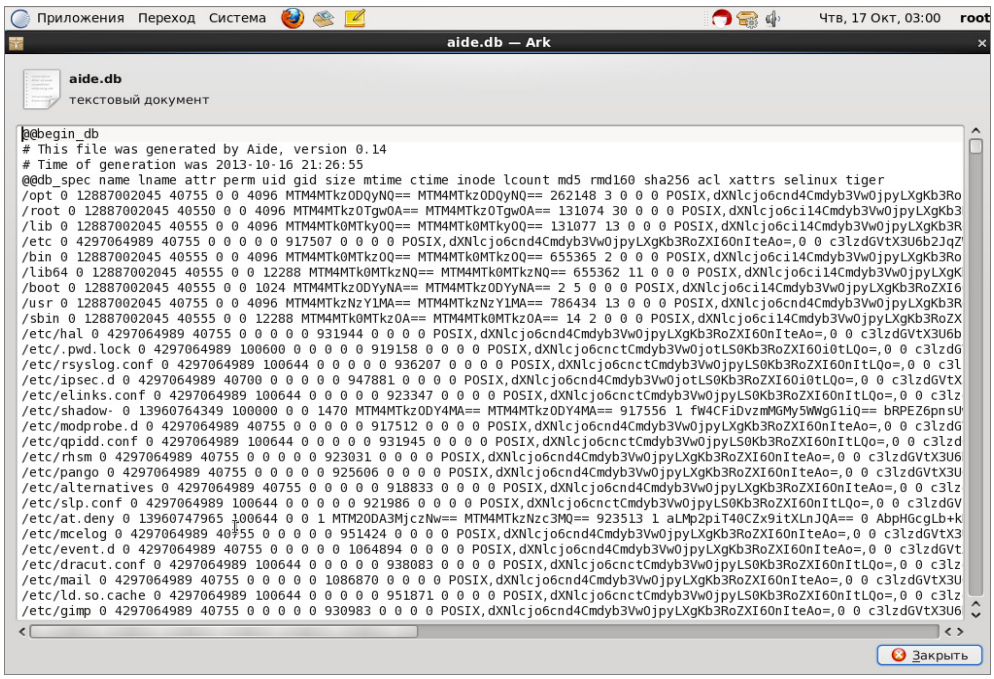


Рисунок 193 - Результат проверки в файле aide.db.gz

ПРИЛОЖЕНИЕ

ПЕРЕЧЕНЬ ПРОГРАММНЫХ ПАКЕТОВ, НЕОБХОДИМЫХ ДЛЯ ФУНКЦИОНИРОВАНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

№	Наименование программного пакета
1	apr-util-ldap
2	bind-dyndb-ldap
3	checkpolicy
4	compat-openldap
5	initscripts
6	ipa-server-selinux
7	iptables
8	iptables-devel
9	iptables-ipv6
10	kernel
11	kernel-devel
12	kernel-firmware
13	kernel-headers
14	krb5-server-ldap
15	ldapjdk
16	libselinux
17	libselinux-devel
18	libselinux-python
19	libselinux-ruby
20	libselinux-utils
21	libsemanage
22	mod_authz_ldap
23	module-init-tools
24	nss-pam-ldapd
25	openldap
26	openldap-clients
27	openldap-devel
28	openldap-servers

29	pam_ldap
30	php-ldap
31	pki-selinux
32	policycoreutils
33	policycoreutils-gui
34	policycoreutils-newrole
35	policycoreutils-python
36	policycoreutils-sandbox
37	python-ldap
38	qemu-kvm
39	qemu-kvm-tools
40	rdesktop
41	selinux-policy
42	selinux-policy-minimum
43	selinux-policy-mls
44	selinux-policy-targeted
45	setup
46	spice-client
47	spice-glib
48	spice-gtk
49	spice-gtk-python
50	spice-server
51	spice-vdagent
52	spice-xpi
53	system-config-firewall
54	system-config-firewall-base
55	system-config-firewall-tui
56	util-linux-ng

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

API	Application Programming Interface (Интерфейс программирования приложений)
ACL	Access Control List (Список контроля доступа)
AMTU	Abstract Machine Test Utility (Абстрактная машинная тестовая утилита)
AIDE	Advanced Intrusion Detection Environment (Среда обнаружения вторжений)
BIOS	Basic Input/Output System (Базовая система ввода-вывода)
CA	Certification authority (Центр сертификации)
CPU	Central Processing Unit (Центральное процессорное устройство)
CIFS	Common Internet File System (Общая файловая система для Интернет)
DN	Distinguished Name (Уникальное имя)
DNS	Domain Name System (Система доменных имён)
DAC	Discretionary Access Control (Дискреционное управление доступом)
DCM	Data Center Manager (Intel) (Управлениеданными центра Intel)
DHCP	Dynamic Host Configuration Protocol (Протокол динамической настройки узла)
ESP	EFI System Partition (Системный раздел EFI)
EPT	Extended Page Tables (Расширенная поддержка таблицы страниц)
FTP	File Transfer Protocol (Протокол передачи файлов)
GID	Group Identifier (Идентификаторы группы)
GFS	Google File System (Распределенная файловая система)
GMT	Greenwich Mean Time (Среднее время по Гринвичу)
GPU	Graphical Processing Unit (Модуль графического процесса)
GRUB	GRand Unified Bootloader (Загрузчик операционной системы)
GUID	Globally Unique Identifier (Глобальный уникальный идентификатор)
HTTP	HyperText Transfer Protocol (Протокол передачи гипертекста)
HTTPS	HyperText Transfer Protocol Secure (Протокол, поддерживающий шифрование)
IPA	International Phonetic Alphabet (Международный фонетический алфавит)
ID	Identifier (Идентификатор)
ICMP	Internet Control Message Protocol (Протокол межсетевых управляющих сообщений)
IP	Internet Protocol (Межсетевой протокол)
KDC	Key Distribution Center (Центр распространения ключей)
KVM	Kernel-based Virtual Machine (Виртуальная машина на базе ядра)

LDAP	Lightweight Directory Access Protocol (Облегчённый протокол доступа к каталогам)
LAF	Lightweight Audit Framework (Платформа аудита)
MLS	Multilevel Security (Многоуровневая система безопасности)
MCS	Multi-categories security (Многокатегорийная система)
MAC	Mandatory access control (Полномочный контроль доступа)
MTA	Mail Transport Agent (Агент доставки почты)
MUA	Mail User Agent (Почтовый агент пользователя)
NIS	Network Information Service (Информационная служба сети)
NFS	Network File System (Протокол сетевого доступа к файловым системам)
NPT	Nested Page Tables (Поддержка таблицы вложенных страниц)
NM	Node Manager (Менеджер узла)
PAM	Pluggable Authentication Modules (Подключаемые модули аутентификации)
PID	Process IDentifier (Идентификатор процесса)
PIE	Position-Independent Executable (Позиции независимых исполнимых программ)
PIO	Programmed input/output (Программных инструкций ввода/вывода)
PCI	Peripheral component interconnect (Взаимосвязь периферийных компонентов)
QEMU	Quick EMUlator (Эмулятор аппаратного обеспечения различных платформ)
RBAC	Role Based Access Control (Управление доступом на основе ролей)
SSSD	System Security Services Daemon (Демон "Сервисов безопасности системы")
SELinux	Security-Enhanced Linux (Linux с улучшенной безопасностью)
SVM	Secure Virtual Machine (Безопасная виртуальная машина)
SAN	Storage Area Network (Сеть хранения данных)
SMB	Server Message Block (Блок серверных сообщений)
SMTP	Simple Mail Transfer Protocol (Простой протокол передачи почты)
SSH	Secure Shell (Безопасная оболочка)
TLS	Transport Layer Security (Безопасность транспортного уровня)
TE	Type Enforcement (Соблюдение типов)
TTL	Time to live (Время жизни)
TOS	Type of Service (Тип услуги)
UID	User Identifier (Идентификаторы пользователя)
URI	Uniform Resource Identifier (Унифицированный идентификатор ресурса)
URL	Uniform Resource Locator (Единообразный локатор ресурса)

USB	Universal Serial Bus (Универсальная последовательная шина)
UDP	User Datagram Protocol (Протокол пользовательских датаграмм)
UNIX	Uniplex Information and Computing Services (Сетевая операционная система)
VT	Virtualization Technology (Технология виртуализации)
VFAT	Virtual File Allocation Table (Виртуальная таблица размещения файлов)
WINS	Windows Internet Name Service (Служба имён Windows Internet)
ВМ	Виртуальная машина
ИТ	Информационные технологии
ОС	Операционная система
ПО	Программное обеспечение
ПЭВМ	Персональная электронно-вычислительная машина

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ докум.	Входящий № сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					

Изм.	Лист	№ докум	Подп	Дата