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.

Изм.	Лист	№ докум	Подп	Дата

# СОДЕРЖАНИЕ

1	BB	ведение	6
2	УС	СТАНОВКА И ОБНОВЛЕНИЕ СИСТЕМЫ	7
	2.1	Установка системы	
	2.2	Обновление системы	
3	ИД	ІЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ	
	3.1	Основные сведения	
	3.2	Приложение "Конфигурация аутентификации"	
	3.3	ПРИЛОЖЕНИЕ "KERBEROS AUTHENTICATION CONFIGURATION"	
	3.4	Приложение "Менеджер пользователей"	
	3.5	Утилита снаде	
4	УП	ІРАВЛЕНИЕ ДОСТУПОМ	
	4.1	Основные сведения	
	4.2	Определение доступа к файлам и папкам	
	4.3	Списки контроля доступа	
	4.4	Приложение "Менеджер пользователей"	
	4.5	Утилиты командной строки	
	4.6	Приложение "Администрирование SELinux"	
	4.7	Конфигурационный файл /etc/sudoers	
	4.8	Библиотеки РАМ	
	4.9	Приложение "Хранитель экрана"	
	4.10	ПОДСИСТЕМА ЯДРА RFKILL	
	4.11	Приложение "Настройка Kickstart"	81
	4.12	ФАЙЛ /ETC/ISSUE	83
	4.13	Метки безопасности	85
5	УП	ІРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ	
	5.1	Основные сведения	
	5.2	УТИЛИТА СНАGE	
	5.3	Команда Снғл	
	5.4	УТИЛИТА CHSH	
	5.5	УТИЛИТА USERADD	
	5.6	УТИЛИТА USERMOD	
	5.7	УТИЛИТА USERDEL	
	5.8	УТИЛИТА GROUPADD	
	5.9	УТИЛИТА GROUPMOD	
	5.10	УТИЛИТА GROUPDEL	

Изм.	Лист	№ докум	Подп	Дата

	5.11	УТИЛИТА СНСАТ	101
	5.12	УТИЛИТА CHCON	101
	5.13	УТИЛИТА СНЕСКРОLICY	102
	5.14	УТИЛИТА LOAD_POLICY	103
	5.15	УТИЛИТА RESTORECON	103
	5.16	УТИЛИТА RESTORECOND	104
	5.17	Утилита semodule	104
	5.18	УТИЛИТА SETENFORCE	105
	5.19	Утилита setfiles	106
	5.20	Утилита AIDE	107
	5.21	Утилита AMTU	107
	5.22	УТИЛИТА SUDO	109
	5.23	УТИЛИТА GETFACL	111
	5.24	УТИЛИТА SETFACL	112
	5.25	Утилита нwclock	113
	5.26	УТИЛИТА RNANO	113
	5.27	Приложение «Администрирование SELinux»	116
	5.28	Конфигурационный файл /etc/sudoers	117
	5.29	ПРИЛОЖЕНИЕ «МЕНЕДЖЕР ПОЛЬЗОВАТЕЛЕЙ»	119
	5.30	Средства управления аудитом	120
	5.31	ПРИЛОЖЕНИЕ «ДАТА И ВРЕМЯ»	121
6	АУД	ИТ БЕЗОПАСНОСТИ	. 122
	61		122
	6.2	Конфигурационные файлы	122
	6.3		122
	6.4	VTUIUTA AUSERCH	123
	6.5		131
	6.6		132
	6.7	Приложение «Алминистрирование SELinux»	135
	6.8	Приложение "Audit Logs"	136
	6.9	ПРИЛОЖЕНИЕ "KsystemLog"	140
	6.10	Лоступ к ланным аулита	140
7	2411		141
'	ЭАЦ	цита от выполнения в едопосного п от гаммного обесне чения	. 141
	7.1	Основные сведения	141
	7.2	ПРИЛОЖЕНИЕ "HACTPOЙKA KICKSTART"	142
	7.3	ВСТРОЕННЫЕ СРЕДСТВА И НАСТРОЙКИ	142
	7.4	УТИЛИТА SUDO	143
	7.5	Приложение "Менеджер пользователей"	143
	7.6	ПРИЛОЖЕНИЕ "НАСТРОЙКА МЕЖСЕТЕВОГО ЭКРАНА"	144
		Изм. Лист № докум Полп Лата	

	7.7	ПРИЛОЖЕНИЕ "ХРАНИТЕЛЬ ЭКРАНА"	
,	7.8	Надежные метки времени	
,	7.9	Утилита АМТU	
,	7.10	Менеджер пакетов <b>RPM</b>	
	7.11	Анализаторы трафика	
8	<b>3A</b> ]	ЩИТА СРЕДЫ ВИРТУАЛИЗАЦИИ	159
	8.1	Основные сведения	
	8.2	Утилита virsh	
	8.3	УТИЛИТА QEMU-IMG	
	8.4	Утилита ls	
	8.5	УТИЛИТА IPTABLES	
	8.6	Утилита пр	
	8.7	УТИЛИТЫ GETFATTR И SETFATTR	
	8.8	Подсистема sVirt	
	8.9	Приложение "Конфигурация аутентификации"	
9	ФИ	ІЛЬТРАЦИЯ ПАКЕТОВ И МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ	168
	9.1	Основные сведения	
	9.1 9.2	Основные сведения Приложение "Настройка Kickstart"	
	9.1 9.2 9.3	Основные сведения Приложение "Hactpoйka Kickstart" Подсистема Netfilter	
	9.1 9.2 9.3 9.4	Основные сведения Приложение "Hactpoйka Kickstart" Подсистема Netfilter Утилита iptables	
	9.1 9.2 9.3 9.4 9.5	Основные сведения Приложение "Hactpoйka Kickstart" Подсистема Netfilter Утилита iptables Утилита iptables-save	
	9.1 9.2 9.3 9.4 9.5 9.6	Основные сведения Приложение "Hactpoйka Kickstart" Подсистема Netfilter Утилита iptables Утилита iptables.save Утилита iptables-save	
	9.1 9.2 9.3 9.4 9.5 9.6 9.7	Ochobhыe сведения Приложение "Hactpoйka Kickstart" Подсистема Netfilter Утилита iptables Утилита iptables-save Утилита iptables-save Утилита iptables-restore Утилита ipfables	
	9.1 9.2 9.3 9.4 9.5 9.6 9.7 9.8	Основные сведения         Приложение "Настройка Kickstart"         Подсистема Netfilter         Утилита iptables         Утилита iptables-save         Утилита iptables-restore         Утилита iptables	
	9.1 9.2 9.3 9.4 9.5 9.6 9.7 9.8 9.9	Основные сведения         Приложение "Настройка Kickstart"         Подсистема Netfilter         Утилита iptables         Утилита iptables-save         Утилита iptables-restore         Утилита ipfables         Утилита iptables         Утилита iptables         Утилита iptables         Утилита iptables         Утилита iptables         Утилита iptables         Утилита ipfables         Утилита ipfables         Утилита ipfables         Приложение "Настройка межсетевого экрана"	
10	9.1 9.2 9.3 9.4 9.5 9.6 9.7 9.8 9.9 <b>OE</b>	Основные сведения	
10	9.1 9.2 9.3 9.4 9.5 9.6 9.7 9.8 9.9 <b>OE</b> 10.1	Основные сведения	
10	9.1 9.2 9.3 9.4 9.5 9.6 9.7 9.8 9.9 <b>OE</b> 10.1 10.2	Основные сведения	
10	9.1 9.2 9.3 9.4 9.5 9.6 9.7 9.8 9.9 <b>OE</b> 10.1 10.2 10.3	Основные сведения	168 169 170 172 178 178 178 179 179 182 191 191 191 193
10	9.1 9.2 9.3 9.4 9.5 9.6 9.7 9.8 9.9 <b>ОБ</b> 10.1 10.2 10.3 <b>РИЛО</b>	Основные сведения	168 169 170 172 172 178 178 178 179 179 182 191 191 191 193 199

Изм.	Лист	№ докум	Подп	Дата

#### 1 ВВЕДЕНИЕ

МСВСфера 6.3 APM – 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.

Изм.	Лист	№ докум	Подп	Дата

#### 2 УСТАНОВКА И ОБНОВЛЕНИЕ СИСТЕМЫ

#### 2.1 Установка системы

Для установки МСВСфера 6.3 АРМ необходимо выполнить следующую последовательность действий<sup>\*</sup>.

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

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

Изм.	Лист	№ докум	Подп	Дата

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 «ОК», 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

Изм.	Лист	№ докум	Подп	Дата

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

Welcome to MSUSphere for x86_64	
Media eje	cted
The disc currentl your drive was ej	y inserted to ected. Press
UK to continue.	
ОК	
<tab>/<alt-tab> between elements   <spa< td=""><td>ce&gt; selects   <f12> next screen</f12></td></spa<></alt-tab></tab>	ce> selects   <f12> next screen</f12>

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

7. Установочная система загрузит графический модуль.

Media Detected Found local installation media	

Рисунок 7 – Загрузка графического модуля

Изм.	Лист	№ докум	Подп	Дата

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

Изм.	Лист	№ докум	Подп	Дата

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

What language would you like to use during the installation process?	
Malayalam (മലയാളം)	<u> </u>
Marathi (मराठी)	
Nepali (Nepali)	
Northern Sotho (Northern Sotho)	
Norwegian(Bokmål) (Norwegian(Bokmål))	
Oriya (ଓଡ଼ିଆ)	
(فارسی) Persian	
Polish (polski)	
Portuguese (Português)	
Portuguese(Brazilian) (Português (Brasil))	
Punjabi (ਪੰਜਾਬੀ)	
Romanian (Română)	
Russian (Русский)	
Serbian (српски)	
Serbian(Latin) (srpski(latinica))	
Sinhala (	
Slovak (Slovenčina)	
Slovenian (slovenščina)	
Spanish (Español)	=
Swedish (Svenska)	
Tajik (Tajik)	
Tamil (தமிழ்)	
Telugu (ອີຍນາັນ)	
Turkish (Türkçe)	
Ukrainian (Українська)	~
	<b>♦</b> Back

Рисунок 10 – Выбор языка

11. После этого будет предложено выбрать раскладку клавиатуры.

анадская (французскии)	
Сорейская	
Татиноамериканская	
Лакедонская	
lемецкая	
łемецкая (latin1)	
leмецкая (latin1, без мертвых клавиш)	
юрвежская	
Тольская	
Іортугальская	
умынская	
усская	
Сербская	
Сербская (Латинский)	
Словацкий (qwerty)	
Словенская	
Соединенное Королевство	
урецкая	
′краинская	
Финская	
Финская (latin1)	
Французская	
Doanuvsckas (latin1)	

Рисунок 11 – Выбор раскладки клавиатуры

Изм.	Лист	№ докум	Подп	Дата

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

акой тип устройств будет использоваться при установке?		
Станлартные накопители		
Стандартные накончение на стандартных наколителях. Этот выбор полходит, если вы не	•	
установка или оповление на стандартнах накопителих. Этот выобр подходит, если вы не	<u> </u>	
Jucpenia, Rakon Buphani elegger Baloparia.		
Checkwardshale hakoliniezin		
2 позволяет установить и обновить устройства зай благаде неа нескотку, дооавить диски нсое, ISCS1 запазт, устройства, котроно истановании доджен будат продистить.		
посот, стер и задать устроиства, которые установщик должен будет пропустить.		
		а пазад 🔰 🗖 Дал

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.

На устройстве не обнаружены разделы и файловые системы. Возможно, это устройство <b>пустое, неразмеченное</b> или <b>виртуальное</b> . Если это не так, при продолжении установки данные, находящиеся на этом устройстве, могут быть утрачены. Для переотвращения потери данных это устройство можно исключить из установки. Вы уверены, что это устройство не содержит важные данные?	ATA VMware Virtual I           20480.0 MB         pci-0000:00:07.1-scsi-0:0:0:0
☑ Применить мой выбор ко всем устройствам с нераспознанными разделами и файловыми системами Да, удалить данные Нет, сохранить данные	Возможно, это устройство <b>пустое, неразмеченное</b> или <b>виртуальное</b> . Если это не так, при пордолижении установки данные, находящиеся на этом устройстве, могут быть утрачены. Для предотвращения потери данных это устройство можно исключить из установки. Вы уверены, что это устройство не содержит важные данные? ☑ Применить мой выбор ко всем устройствам с нераспознанными разделами и файловыми системами 且а, удалить данные

Рисунок 13 – Окно-предупреждение

Изм.	Лист	№ докум	Подп	Дата

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

Присвойте этому компьютеру имя, которое будет использоваться для его идентификации в сети.	
Имя узла: focalhost.localdomain	
	k
Настроить сеть	
	<u>         Назад</u> <u>         Далее</u>

Рисунок 14 – Имя компьютера

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

Присвойте этому комп будет использоваться сети.	ьютеру имя, которое для его идентификации	В			
Имя узла: localhost.localdomain					
		Сетевые соединения			
	📄 Проводные 📄 Е	еспроводные 🎇 Мобильные 🧟	VPN 🗐 DSL		
	Название	Последнее подключение	Добавить		
	System culo	не овло подолочения	Изменить		
			Удалить		
			Закрыть		
Настроить сеть					
				<del>व</del> <u>Н</u> азад	📫 Далее

Рисунок 15 – Настройка сети

Изм.	Лист	№ докум	Подп	Дата

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.

учетная запис	ь гоот используется для вания системы		
Введите парол	ь пользователя root.		
Пароль root:	•••••	]	
Подтвердите:	•••••	j	
		<b>—</b> Назад	📄 Далее
			- Havee

Рисунок 17 – Пароль администратора

Изм.	Лист	№ докум	Подп	Дата



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

Изм.	Лист	№ докум	Подп	Дата

# ЦАУВ.14001-01 91 01

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

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.

Стандартная установка МСВСфера 6.3 АРМ включает минимальный набор программ. По желанию можно выбрать другой набор программ.	
• Рабочий стол	
О Минимальная настольная установка	
О Рабочая станция веб-разработки	
Рабочая станция разработки программ	
О Минимальный	
*	
зыберите дополнительные репозитории для установки ПО.	
☑ MSVSphere 6.3 ARM	
Можно изменить набор пакетов сейчас или после завершения установки с помощью специальной программы управления пакетами.	
○ <u>Н</u> астроить позже	

Рисунок 20 – Выбор наборов программ

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

вазовая система	🎒 🗖 Веб-сервер
Серверы	💮 🗆 Веб-сервлеты
Веб-службы	👩 🗆 Поддержка PHP
Базы данных	🗿 🗆 Программная инфраструктура TurboGears.
Управление системой	
Виртуализация	
Рабочие столы	
Приложения	
Программирование	
Языки	
<b>k</b>	
Позволяет системе функционироват	ть в качестве веб-сервера и выполнять веб-приложения Perl и Python.
Позволяет системе функционироват	ть в качестве веб-сервера и выполнять веб-приложения Perl и Python.
Позволяет системе функционироват	ть в качестве веб-сервера и выполнять веб-приложения Perl и Python.
Позволяет системе функционироват	ть в качестве веб-сервера и выполнять веб-приложения Perl и Python.
Позволяет системе функционироват	ть в качестве веб-сервера и выполнять веб-приложения Perl и Python.
Позволяет системе функционироват	ть в качестве веб-сервера и выполнять веб-приложения Perl и Python. Дополнительные пакеты
Позволяет системе функционироват	ть в качестве веб-сервера и выполнять веб-приложения Perl и Python. Дополнительные пакеты
Позволяет системе функционироват	ть в качестве веб-сервера и выполнять веб-приложения Perl и Python.

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

Изм.	Лист	№ локум	Подп	Дата

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».

Добро пожаловать Информация о лицензии > Пользователь Дата и время	Пользов Требуется создать пол административного) ис необходимые данные.	атель взователя для повседневного (не пользования системы. Для этого введите	
Kdump	<u>И</u> мя пользователя:	1	
100 B	Полное им <u>я</u> :	Иван	
	Пароль:	•••••	
	По <u>д</u> твердите пароль:	•••••	
ß	Если требуется исполь например Кеrberos или аутентификация». Сетевая аут <u>е</u> нтифика Для настройки других нажните кнопку «Допо <u>Дополнительно</u>	зовать проверку подлинности по сети, NIS, нажиите кнопку «Сетевая щия параметров (домашмего каталога, UID) лиительно».	Назад <u>В</u> лерёд

Рисунок 26 – Создание пользователя для повседневной работы

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

Добро пожаловать Информация о лицензии Пользователь • Дата и время Кdump	рать мация о ми затель время с дата и время пожалуйста, установите дату и время системы. Пожалуйста, установите дату и время системы. Пата и время Текущие дата и время: Пид 04 Фев 2013 14:32:27 Сунхронизация даты и времени по сети Установка системной даты и времени вручную:								
	<u>Д</u> ата						Время		
	< Φe	враль	>		< 20	013 >	Часы: 14		
	Пнд	Втр Ср	д Чтв	Птн	Сбт	Вск	Минуты : 31		
	28	29 3	0 31	1	2	3			
	4	5 6	7	8	9	10	секунды: 30 🔽		
	11	12 1	3 14 0 21	22	23	24			
	25	26 2	7 28						
	4			8					
							Назад Вперёд		

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 Кdump



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 уит или при помощи приложения «Обновление программ».

Обновление с компакт-диска с использованием команды уum 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.

Изм.	Лист	№ докум	Подп	Дата

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.

Изм.	Лист	№ докум	Подп	Дата

#### 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

Изм.	Лист	№ докум	Подп	Дата

24

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.

Конфигурация ауте	нтификации ×			
Идентификация и аутентификация Дополнительн	ые параметры			
Настройка учётной записи пользователя				
<u>Б</u> аза данных учётных записей пользователей:	Только локальные учётные записи			
	LDAP			
	IPAv2			
	NIS			
	Winbind			
Настройка аутентификации				
С <u>п</u> особ аутентификации:	Пароль			
<u>В</u> осстановить	О <u>т</u> менить <u>П</u> рименить			

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

Изм.	Лист	№ докум	Подп	Дата

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.

1	🖢 Конфигурация аутентификации >
1	Идентификация и аутентификация Дополнительные параметры
	Настройка учётной записи пользователя
	<u>Б</u> аза данных учётных записей пользователей: LDAP
	Базовое DN для поиска LDAP:
	<u>С</u> ервер LDAP:
	Использовать <u>T</u> LS для шифрования соединений
	🧱 Загрузить сертификат СА
	Настройка аутентификации
	С <u>п</u> особ аутентификации: Пароль LDAP
	Восстановить Отменить Применить

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.

Изм.	Лист	№ докум	Подп	Дата

ЦАУВ.14001-01 91 01

💩 Конфигурация аутентификации
Идентификация и аутентификация Дополнительные параметры
Для подключения домена к IPAv2 нажмите «Войти в домен».
Настройка учётной записи пользователя
База данных учётных записей пользователей: IPAv2 🗘
<u>Д</u> омен IPA:
О <u>б</u> ласть IPA:
<u>С</u> ервер IPA:
Не настраивать NTP
🔚 Войти в домен
Настройка аутентификации
С <u>п</u> особ аутентификации: Пароль IPAv2 🗘
<u>Восстановить</u> <u>Применить</u>

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.

💩 Конфигурация аутен	тификации ×
<u>И</u> дентификация и аутентификация <u>Д</u> ополнительн	ые параметры
Настройка учётной записи пользователя	
База данных учётных записей пользователей:	NIS
<u>Д</u> омен NIS: С <u>е</u> рвер NIS:	
Настройка аутентификации	
С <u>п</u> особ аутентификации:	Пароль NIS
Восстановить	О <u>т</u> менить <u>П</u> рименить

Рисунок 36 - Окно настройки аутентификации с использованием системы NIS

Изм.	Лист	№ докум	Подп	Дата

27

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-cepвер; указываются контроллеры домена и оболочка для настройки учётной записи пользователя Windows. Установка флага «Разрешить автономный вход» позволяет сохранять аутентификационную информацию в локальном кэше.

🚈 Конфигурация аутентификации 🗙				
Идентификация и аутентификация	<u>Д</u> ополнительны	е параме	етры	
Настройка учётной записи пользователя				
<u>Б</u> аза данных учётных записей по	льзователей:	Winbind		\$
<u>Д</u> омен Winbind:	MYGROUP			
<u>М</u> одель защиты:	user			\$
<u>О</u> бласть ADS Winbind:				
Ко <u>н</u> троллеры домена Winbind:				
О <u>б</u> олочка шаблона:	/bin/false			
<u>Р</u> азрешить автономный вхо	рд			
	Войти в до	мен		
Настройка аутентификации				
С <u>п</u> особ аутентификации:		Пароль	Winbind	\$
Восстановить			О <u>т</u> менить	Применить

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;

Изм.	Лист	№ докум	Подп	Дата

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

💩 Конфи	игурация аутентификации
Идентификация и аутентификация	Дополнительные параметры
Опции локальной аутентификац	Тии
Включить поддержку <u>ч</u> тения с	отпечатков
Включить <u>л</u> окальное управлен	ние доступом
Подсказка: Управление осущест	твляется в /etc/security/access.conf.
Ал <u>г</u> оритм хэширования пароля:	SHA512 \$
<b>Другие опции аутентификации</b> <ul> <li>Создавать <u>д</u>омашние каталоги</li> </ul>	и при первом входе
Опции аутентификации смарт-к	арт
Включить поддержку смарт-ка	арт
Подсказка: Смарт-карты поддер возможности журналирования в л централизованно управляемых уч	рживают локальных и чётных записях.
Восстановить	О <u>т</u> менить Применить

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).

Изм.	Лист	№ докум	Подп	Дата

ЦАУВ.14001-01 91 01

👎 Kerb	eros Authentication Configuration $$ $$ $$ $$ $$ $$ $$ $$
Kerberos	Applet
Kerber	os User
R	Kerberos principal:
	PKINIT:
	Userid:
	<u>B</u> rowse
	X509 trust anchors:
	<u>B</u> rowse
Ticket (	Options
	Requested Kerberos tickets should be:
	forwardable
	renewable
<u>С</u> правк	а <u>З</u> акрыть

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.

Изм.	Лист	№ докум	Подп	Дата

30

Таблица 1. Действительные дескрипторы служб

Дескриптор службы	Служба
host	Telnet, RSH, SSH
nfs	NFSv4 (с поддержкой Kerberos)
НТТР	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).

🕅 Kerb	eros Authentication Configuration
Kerberos	Applet
Kerber	os User
R	Kerberos principal:
	PKINIT: Userid:
	PKCS11:/usr/lib/opensc. Browse
	X509 trust anchors:
	<u>B</u> rowse
Ticket (	Options
	Requested Kerberos tickets should be:
	forwardable
	renewable
	proxiable
<u>С</u> правка	а <u>З</u> акрыть

Рисунок 40 - Использование смарт-карт для аутентификации

Изм.	Лист	№ докум	Подп	Дата

РКІNІТ 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»

Изм.	Лист	№ докум	Подп	Дата

#### 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).

8	Менеджер пользователей	_ 🗆 ×
<u>Ф</u> айл <u>П</u> ра	вка <u>С</u> правка	
(	R 🚯 R R 🛛 💿	
Добавить г	пользователя Добавить группу Свойства Удалить Обновить Справка	
	🔹 Свойства пользователя _ 🗆 🗙	
	Данные пользователя <u>С</u> ведения об учётной записи <u>С</u> ведения о пароле <u>г</u> руппы	гь фильтр
Пользовате	Ограничить срок лействия пароля	ĺ
Имя пользо		й каталог
xguest	Смена разрешена через (дней): 0	Jest
user	Смена требуется через (дней): 99999	er
	вудет предупрежден за (днеи).	
	Будет заблокирован через (дней): -1	
	🗌 Изменить пароль при следующей авторизации	
	Дата последнего изменения пароля: 20.12.2013	
		-
	О <u>т</u> менить <u>О</u> К	
×.		

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".

Изм.	Лист	№ докум	Подп	Дата

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".

🔘 Приложения	Переход Система 🎯 🕸 🗾	чтв, 9 Янв, 21:27 <b>гоот</b>
Компьютер	🙆 Менеджер пользователей	_ = ×
	<u>Ф</u> айл <u>П</u> равка <u>С</u> правка	
Ломашняя па		
пользователя	Добавить пользователя Добавить группу Свойства Удалить Обновить Справка	
	🏝 Свойства пользователя 💶 🗆 🗧	
	Ланные пользователя Сведения об учётной записи Сведения о пароде Группь	гь фильтр
Корзина	Пользовате Состаницить спок лействия учётной записи	
		й каталог
	хочеят	lest
	user Докальный пароль заблокирован	ar
	Отменить	
	۵. III	
🛞 Менеджер п	пользователей 🛛 🙆 Свойства пользователя	

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".

Изм.	Лист	№ докум	Подп	Дата

ЦАУВ.14001-01 91 01

🔘 Приложения	Переход Система 🍪	۸ 🖉		🚨 🎪	Чтв, 9 Янв, 21:25 <b>гоот</b>
Компьютер					
	42	Менеджер пол	ьзователей		_ = ×
命	<u>Ф</u> айл <u>П</u> равка <u>С</u> правка				
Домашняя па	<b>P</b>	🛔 Добавить нового	пользователя _ 🗆 🗙	0	
пользователя	Добавить пользователя	<u>И</u> мя пользователя:		Справка	
		Полное и <u>м</u> я:		Применить	фильтр
Корзина	Пользователи Группы	<u>П</u> ароль:			
	Имя пользователя ID п	Подтвердите пароль:		ка Домашний	каталог
	xguest 500	-	(hin the sh	h /home/xgue	st
	user 501	Оболочка:	/bin/bash 🗸	h /home/user	
	k	<ul> <li>☑ Создать домашний кат Домашний каталог: [// ☑ Создать частную [рупп</li> <li>☑ Указать ID польдовате.</li> <li>☑ Укажите ID группы вру</li> </ul>	алог home/ hy для пользователя ля вручную: 503 \$ 503 \$ 0 Iменить <u>QK</u>		
	<u>(</u>		11		
🔞 Менеджер г	юльзователей 🛛 🙆 Добаві	ить нового пользо			

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.

🔘 Приложения	Переход Система ຢ 🕸 🗾	🚨 🕼	Чтв, 9 Янв, 21:32	2 root
Компьютер				
	🐵 Менеджер пользователей		_ = ×	
合	<u>Ф</u> айл <u>П</u> равка <u>С</u> правка			
Ломашняя па		Ø		
пользователя	Добавить пользователя Добавить группу Свойства Удалить Обновить	Справка		
	Фильтр <u>п</u> оиска:	Применит	ь фильтр	
Корзина	Пользователи Группы			
	Имя пользователя ID пол	а Домашниі	й каталог	
	xguest 500 ? Вы деиствительно хотите ygaлить пользователя «xguest»? ash	ı /home/xgu	est	
	user 501 sh	n /home/use	r	
	Удалить домашний каталог пользователя ✓ xguest («/home/xguest»), буфер почты («/var/ spool/mail/xguest») и временные файлы. <u>Н</u> ет Да			
🛞 Менеджер г	тользователей			

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 (/).

📧 root@localhost:~/Рабочий стол	-	×
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка		
[root@localhost Рабочий стол]# python		^
Python 2.6.6 (r266:84292, May 11 2013, 09:23:13)		
[GCC 4.4.6 20120305 (Red Hat 4.4.6-4)] on linux2		
Type "help", "copyright", "credits" or "license" for more information.		
>>> import crypt		_
<pre>&gt;&gt;&gt; passwduser2=crypt.crypt('day',"df")</pre>		=
>>> print passwduser2		
df6HChnLfC4eM		
>>>		
		~

Изм.	Лист	№ докум	Подп	Дата

36
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.

🖂 root@localhost:~/Рабочий стол	_ 0	⊐ x			
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка					
root@localhost Рабочий стол]# passwd user2					
мена пароля для пользователя user2.					
Новый пароль :					
овторите ввод нового пароля :					
passwd: все токены проверки подлинности успешно обновлены.					
[root@localhost Рабочий стол]#		~			

Изм.	Лист	№ докум	Подп	Дата

### 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;

Изм.	Лист	№ докум	Подп	Дата

- 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 РАМ;
- приложение "Хранитель экрана";
- приложение "Настройка Kickstart";
- конфигурационный файл /boot/grub/grub.conf;
- подсистемы ядра RFKill;
- файл /etc/issue;
- метки безопасности.

Изм.	Лист	№ докум	Подп	Дата

### 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 гооt 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»

Изм.	Лист	№ докум	Подп	Дата

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;

	usr	- • ×	
<u>Ф</u> аил <u>П</u> равка <u>В</u>	ид Пере <u>х</u> од <u>С</u> правка		Свойства 1 х
		Основные Эмблемы Пр	ава Заметки
1	2	<u>В</u> ладелец:	root
		Доступ к папке:	Создание и удаление файлов
etc	games	Доступ к файлу:	\$
lib	lib64	<u>Г</u> руппа:	root
		Доступ к папке:	Доступ к файлам
local	sbin	Доступ к файлу:	\$
	5	Остальные	
		Доступ к папке:	Только перечисление файлов
src	tmp	Доступ к файлу:	\$
Откры		Выполнение:	Позволять выполнение файла как программы
Документ2	лен (внутри 0 объектов)	<u>К</u> онтекст SELinux:	[∉]usr_t   ≎]
изго «т» выдел	nen (Bhy i pu o oo bek i ob)	Последние изменения:	Срд 09 Окт 2013 14:40:08
		Распространить права	на вложенные файлы
		<u>С</u> правка	Закрыть

«Нет» – нет доступа к выбранной директории.

Рисунок 48 - Определение типа доступа к папке

Изм.	Лист	№ докум	Подп	Дата

42 ЦАУВ.14001-01 91 01

<u>Ф</u> айл <u>П</u> равн	ка <u>В</u> ид Пере <u>х</u> од <u>С</u> пра	usr BKa	>	
1	2	3	4	
Ē	С Файл Правка Вид	1 Пере <u>х</u> од <u>С</u> правка	_ = ×	
bin	Документ1	Документ2		
lib				
sbin		Не уда Файл не	алось показать «/usr/] известного типа	× L/Документ1».
Откры			k	Ōĸ
Докуме	нт1 1 🕶 1 🗸 «Документ2»	выделен		×
usr ✔ «4»	выделен (внутри 0 объек	(тов)	Не удалось показ Файл неизвестного тиг	в <b>ать «/usr/1/Документ2».</b> <sup>1а</sup>
				<u>O</u> K

Рисунок 49 – Тип доступа "Только перечисление файлов"

## 4.3 Списки контроля доступа

МСВСфера 6.3 APM 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.

Изм.	Лист	№ докум	Подп	Дата

Image: state s	_ = ×
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка	
<pre>[root@localhost etc]# getfacl aide.conf # file: aide.conf # owner: root # group: root user::rwx user:user:rwx group::r-x group:user:rwx mask::rwx other::r-x</pre>	

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 группывладельца (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).

Изм.	Лист	№ докум	Подп	Дата

Для установки компонента ACL\_USER для файла, необходимо воспользоваться командой setfacl.

setfacl -<oпции> <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:---

Изм.	Лист	№ докум	Подп	Дата

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.

-т Изменяет режимы доступа к файлу (каталогу).

-х 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-х» (рис. 51), тем самым пользователь не будет иметь право на запись файла, но сможет читать и выполнять файл (рис. 52).

root@localhost:/etc	-	×
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка		
<pre>[root@localhost etc]# setfacl -m "u:user:r-x" /etc/aide.conf [root@localhost etc]# getfacl aide.conf # file: aide.conf # owner: root # group: root user::rwx user:user:r-x group::r-x group:user:rwx mask::rwx other::r-x</pre>		

Рисунок 51 - Компонент ACL\_USER для пользователя user установлен в «r-х»

🔘 Приложения Переход Система 👹 🥸 🗾		<u>ن</u> اء	Птн, 15 Ноя, 15:02 <b>user</b>
		alde.conf [только чтение] (/etc) - gedit	_ 0 ×
компьютер	Фаил П	равка вид поиск сервис документы справка	
etc	_ = ×	Открыть 🗸 🖄 Сохранить 🛛 🚔 🕤 Отменить 🖉	2   2 4 4 6   ~
Помещинатрацию Файл Правка Вид Переход Спра	вка 📄 aide.co	inf 🗶	
	@@define @@define	DBDIR /var/lib/aide LOGDIR /var/log/aide	 ≡
yum yum.repos.	d # The lo database	cation of the database to be read. ≔file:@0{DBDIR}/aide.db.gz	
Корвина итс # The	# The lo	cation of the database to be written.	
adjtime aide.conf	#databas #databas	e_out=sql:host:port:database:login_name:passwd:ta e_out=file:aide.db.new _out=file:@@{NPDTB}/aide_db_new_gz	ble
# AL # Na	uatabase	_out=iite.@@{bbbin}/aide.db.new.gz	
aliases aliases.db	# Whether gzip_dbc	r to gzip the output to database ut=yes	
📄 etc 🗸 «aide.conf» выделен (982,7 К	i) # Defaul	t. 5	
	report u	- rl=file:@@{LOGDIR}/aide.log	
	report_u	rl=stdout	
	#NOT IMF #NOT IMF	LEMENTED report_url=mailto:root@foo.com LEMENTED report_url=syslog:LOG_AUTH	~
		Текст У Ширина табуляции: 8 У Стр	р 1, Стлб 1 ВСТ

Рисунок 52 - Демонстрация результата модификации компонента ACL\_USER

Изм.	Лист	№ докум	Подп	Дата

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).

s root@localhost:/etc	_	×
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка		
<pre>[root@localhost etc]# setfacl -m "g:user1:" /etc/aide.conf [root@localhost etc]# getfacl aide.conf # file: aide.conf # owner: root # group: root user::rwx user:user:r-x group::r-x group:user:r-x group:user1: mask::r-x other::r-x</pre>		<u> </u>

Рисунок 53 - Компонент ACL\_ GROUP для группы user1 установлен в «---»

🔘 Приложения Переход Система	👹 🕸 🗾		¢,	Птн, 15 Ноя, 15:24	user1
	еtс <u>Ф</u> айл <u>П</u> равка <u>В</u> ид Переход <u>С</u> правка		×		
Компьютер	vum repos d aditime aide c	conf			
Домашняя папка пользователя useri	aliases	, «/etc/ai	i <b>de.conf</b> ×	×	
Корзина	<u>metc</u> vaide.conf» выделен (982,7 КБ)				

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).

E root@localhost:/etc	-	×
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка		
<pre>[root@localhost etc]# setfacl -m "u:user:rwx" /etc/aide.conf [root@localhost etc]# setfacl -m "m::r" /etc/aide.conf [root@localhost etc]# getfacl aide.conf # file: aide.conf # owner: root # group: root user:rwx user:user:rwx #effective:r group::r-x #effective:r</pre>		~
group:user:r-x #effective:r group:user1: mask::r other::r-x		

Рисунок 55 - Компонент ACL\_USER установлен для пользователя user в значение «rwx» и

компонент ACL\_MASK установлен в «r--»

Изм.	Лист	№ докум	Подп	Дата

47 ЦАУВ.14001-01 91 01



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 «г--» (рис. 57), тем самым пользователю user файл будет доступен только для чтения (рис. 58).

Σ	root@localhost:/etc	_ 🗆 X
<u>Ф</u> айл	і <u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка	
[root [root getfa # fil # own # gro user: group other	<pre>@localhost etc]# setfacl -m "u::r" /home/user/aide/list.txt @localhost etc]# getfacl /home/user/aide/list.txt cl: Removing leading '/' from absolute path names e: home/user/aide/list.txt er: root up: root :r ::r ::r ::r</pre>	

Рисунок 57 - Компонент ACL\_USER\_OBJ установлен для пользователя-владельца user в



значение «r--»

Рисунок 58 - Демонстрация результата модификации компонента ACL\_USER\_OBJ

Изм.	Лист	№ докум	Подп	Дата

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

🗉 root@localhost:/etc .	- C	×
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка		
<pre>[root@localhost etc]# setfacl -m "o::" /etc/aide.conf [root@localhost etc]# getfacl /etc/aide.conf getfacl: Removing leading '/' from absolute path names # file: etc/aide.conf # owner: root # group: root user::rwx group::r-x mask::r-x other::</pre>		~

Рисунок 59 - Компонент ACL\_ОТНЕЯ 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

Изм.	Лист	№ докум	Подп	Дата

# 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.

🙆 Менеджер пользователей _ 🗆 🗙						
<u>Ф</u> айл <u>П</u> равка <u>С</u> правка						
<b>P</b>	💩 Добавить нового	пользователя _ 🗆 🗙				
Добавить пользователя	<u>И</u> мя пользователя:	user3	Сп	равка		
	Полное и <u>м</u> я:	user3		Применить фильтр		
<u>П</u> ользователи <u>Г</u> руппы	Пароль:	***				
Имя пользователя ID г	Подтвердите пароль:	***	ка	Домашний каталог		
xguest 500	0600000	(thin thank is a	h	/home/xguest		
user 501		/bin/bash 🗸	h	/home/user		
user2 503	<ul> <li>✓ Создать домашний ка Домашний каталог: ✓ Создать частную <u>г</u>руг</li> <li>✓ Указать ID поль<u>з</u>овато</li> <li>✓ Укажите ID группы вр</li> </ul>	аталог /home/user3 ппу для пользователя еля вручную: 504 ♀ уучную: 505 ♀ Отменить QK	h	/home/user2		
		.00		>		

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).

Изм.	Лист	№ докум	Подп	Дата

Файл Прав	Менеджер пользователей	- • ×
Добавить п	и строна Строна ользователя Добавить группу Свойства Удалить Обновить Справка	
	🔈 Свойства пользователя _ 🗆 🗙	
	Данные пользователя <u>Сведения об учётной записи</u> <u>Сведения о пароле</u> <u>группы</u>	гь фильтр
<u>П</u> ользовате	Ограничить срок действия пароля	1
Имя пользе		й каталог
xguest	Смена разрешена через (дней): 0	Jest
user	Смена требуется через (дней): 99999	er
user2	Будет предупрежден за (дней): 7	er2
user3	Булет заблокирован через (лней):	era
	Изменить пароль при следующей авторизации	
	дата последнего изменения пароля. 09.01.2014	
	Отменить ОК	
		>

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 гооt, 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).

Изм.	Лист	№ докум	Подп	Дата

51 ЦАУВ.14001-01 91 01

мсво user Пароль: •••	Сфера 6.3 АРМ Греда 6.3 АРМ	
OIM	енить Войти в систему	

Рисунок 64 - Ввод пароля при входе в систему

M user (текущий) пароль UNIX:	СВСфера 6.3 АРМ	
русский (Воссийская Фелерация).		еп. Чтв. 6:02

Рисунок 65 - Ввод текущего пароля

Изм.	Лист	№ докум	Подп	Дата

52 ЦАУВ.14001-01 91 01

М	ССВСфера 6.3 АРМ ССВСфера 6.3 АРМ С О ТМЕНИТЬ ВОЙТИ В СИСТЕМУ	
русский (Российская Федерация) 🗸	GNOME V	🕅 en Чтв 6:03 🕲

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.

22	Менеджер пользователей	_ 🗆 ×
<u>Ф</u> айл <u>П</u> равка <u>С</u> пра	вка	
<b>Б</b> Добавить пользовато	🛃 💽 🦉 🦉	<b>)</b> авка
	Фильтр поиска:	П <u>р</u> именить фильтр
<u>П</u> ользователи <u>Г</u> руг	& X	
Имя пользователя	Выполняются процессы, которые принадлежат	Домашний каталог
xguest	пользователю «user3». Возможно, данный	/home/xguest
user	пользователь все еще работает с системой. Вы лействительно хотите удалить пользователя «user3»?	/home/user
user2		/home/user2
user3	Удалить домашний каталог пользователя user3 («/home/user3»), буфер почты («/var/spool/ mail/user3») и временные файлы. <u>Н</u> ет Да	/home/user3
	•	
	III III III III III III III III III II	

Рисунок 67 - Удаление учетной записи

Изм.	Лист	№ докум	Подп	Дата

#### 4.5 Утилиты командной строки

Модель полномочного контроля доступа МСВСфера 6.3 APM 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.

🗉 root@localhost:~/Рабочий стол	_	×
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка		
[root@localhost Рабочий стол]# sestatus		^
SELinux status: enabled		
SELinuxfs mount: /selinux		
Current mode: enforcing		
Mode from config file: enforcing		_
Policy version: 24		-
Policy from config file: targeted		
[root@localhost Рабочий стол]#		
•		
		~

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.

Изм.	Лист	№ докум	Подп	Дата

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).

📸 config (/etc/selinux) - gedit	_	×
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск С <u>е</u> рвис <u>Д</u> окументы <u>С</u> правка		
🎦 🚍 Открыть 🗸 🏰 Сохранить   🚔   🏐 Отменить 💩   💥 🛙		~
📄 config 🗶		
<pre># This file controls the state of SELinux on the system. # SELINUX= can take one of these three values: # enforcing - SELinux security policy is enforced. # permissive - SELinux prints warnings instead of enforcing. # disabled - No SELinux policy is loaded. SELINUX=enforcing # SELINUXTYPE= can take one of these two values: # targeted - Targeted processes are protected, # mls - Multi Level Security protection. SELINUXTYPE=targeted</pre>		
	PCT	-

Текст 🗸 Ширина табуляции: 8 🗸 Стр 1, Стлб 1 🛛 Ве

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

📧 root@localhost:~/Рабочий стол	_	×
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка		
[root@localhost Рабочий стол]# getenforce		^
Enforcing		=
[root@localhost Рабочий стол]#		_
[root@localhost Рабочий стол]#		~

Рисунок 70 - Использование утилиты getenforce

Изм.	Лист	№ докум	Подп	Дата

Управление режимами работы SELinux можно осуществлять и через параметры ядра Linux. Параметр selinux=0 эквивалентен значению Disabled в конфигурации SELinux, a 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).

E root@localhost:/etc/selinux/targeted	_ 0 X
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка	
[root@localhost targeted]# semanage login -l   grep default defaultunconfined_u s0-s0:c0.c1023	^
<pre>[root@localhost targeted]# [root@localhost targeted]#</pre>	Ξ
[root@localnost targeted]#	~

Рисунок 71 - Определение SELinux-пользователя по умолчанию

На рис. 71 видно, что пользователи системы по умолчанию сопоставлены SELinuxпользователю 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).

E root	@localhost:/etc/selinux/targ	eted	-	×
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> ис	к <u>Т</u> ерминал <u>С</u> правка			
[root@localhost targeted] [root@localhost targeted]	# useradd -Z guest_u user_ # semanage login -l	6		^
Имя входа	Пользователь SELinux	Диапазон MLS/MCS		
default	unconfined u	s0-s0:c0.c1023		
root	unconfined_u	s0-s0:c0.c1023		
system_u	system_u	s0-s0:c0.c1023		
user_5	guest_u	s0		
user 6	guest u	s0		
xguest	xguest_u	s0		Ξ
[root@localhost targeted]	#			~

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\_и вместо определенного по умолчанию SELinux-пользователя.

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

Изм.	Лист	№ докум	Подп	Дата

E root	@localhost:/etc/selinux/targ	jeted _ 🗆	×
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> ис	к <u>Т</u> ерминал <u>С</u> правка		
[root@localhost targeted]	# semanage login -l		^
Имя входа	Пользователь SELinux	Диапазон MLS/MCS	
default root system_u user_5 user_6 xguest [root@localhost targeted] [root@localhost targeted]	unconfined_u unconfined_u system_u guest_u guest_u xguest_u # usermod -Z unconfined_u # semanage login -l	s0-s0:c0.cl023 s0-s0:c0.cl023 s0-s0:c0.cl023 s0 s0 s0 s0 user_5	
Имя входа	Пользователь SELinux	Диапазон MLS/MCS	
default root	unconfined_u unconfined_u	s0-s0:c0.c1023 s0-s0:c0.c1023	
system_u user_5 user_6 xguest [root@localbost_targeted]	system_u unconfined_u guest_u xguest_u # ■	s0-s0:c0.c1023 s0 s0 s0	=

Рисунок 73 - Сопоставление между пользователем системы и SELinux-пользователем

Существует несколько предопределенных профилей SELinux-пользователей. Список данных профилей можно вывести командой semanage user -1 (рис. 74).

E	root@	localhost:/e	etc/selinux/targeted	_ 🗆 🗙
<u>Ф</u> айл <u>П</u> равка	<u>В</u> ид П <u>о</u> иск	<u>Т</u> ерминал	<u>С</u> правка	
[root@localhos	t targeted]#	semanage u	user -l	^
Пользователь Si SELinux	Разметка ELinux Префи	MLS/ KC MCS )	MLS/ /ровень MCS Диапазон	Роли
git_shell_u guest_u root adm_r_system_r	user user user	s0 s0 s0	s0 s0 s0-s0:c0.c1023	git_shell_r guest_r staff_r sys
staff_u adm r system r	user unconfined	s0 r	s0-s0:c0.c1023	staff_r sys
sysadm_u system_u confined r	user user	s0 s0	s0-s0:c0.c1023 s0-s0:c0.c1023	sysadm_r system_r un
unconfined_u confined r	user	s0	s0-s0:c0.c1023	system_r un
user_u xguest_u [root@localhos [root@localhos	user xguest t targeted]# t targeted]#	s0 s0	s0 s0	user_r xguest_r
[root@localhos	t targeted]#	1		~

Рисунок 74 - Предопределенные профили SELinux-пользователей

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

Изм.	Лист	№ докум	Подп	Дата

Σ	root@localhost:/etc/selinux/ta	argeted	_	×
<u>Ф</u> айл <u>П</u> равка <u>В</u> и,	д П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка			
[root@localhost ta	rgeted]# semanage login -l			^
Имя входа	Пользователь SELinux	Диапазон MLS/MCS		
default root system_u	unconfined_u unconfined_u system_u	s0-s0:c0.c1023 s0-s0:c0.c1023 s0-s0:c0.c1023		
user_5 user_6	quest u	50		
xguest [root@localhost ta	xguest_u argeted]#∎	s0		

Рисунок 75 - Вывод списка всех сопоставлений

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

E root(	]localhost:/etc/selinux/targ	eted _ 🗆	×
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск	: <u>Т</u> ерминал <u>С</u> правка		
[root@localhost targeted]	# semanage login -l		^
Имя входа	Пользователь SELinux	Диапазон MLS/MCS	
default root system_u user_5 xguest [root@localhost targeted]a [root@localhost targeted]a	unconfined_u unconfined_u system_u unconfined_u xguest_u # semanage login -d user_5 # semanage login -l	S0-S0:C0.C1023 S0-S0:C0.C1023 S0-S0:C0.C1023 S0 S0	
Имя входа	Пользователь SELinux	Диапазон MLS/MCS	
default root system_u xguest [root@localhost targeted];	unconfined_u unconfined_u system_u xguest_u #	s0-s0:c0.c1023 s0-s0:c0.c1023 s0-s0:c0.c1023 s0	

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.

Изм.	Лист	№ докум	Подп	Дата

57

#### 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 selinuxpolicy-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.

Изм.	Лист	№ докум	Подп	Дата

58

Политика безопасности minimum. Этот режим доступен, если установлен пакет selinuxpolicy-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".

🕈 Администрирование SELinux _ 🗆 🛪					
<u>Ф</u> айл <u>С</u> правка					
Выбор:	Строгий режим по умолчанию	Строгий			
Статус					
Переключатель	Текущий строгий режим	Строгий 🗘			
Присвоение меток файлам	Тип политики по умолчанию:	targeted			
Сопоставление пользователей					
Пользователь SELinux	🗆 🔁 Переразметка при следу	ющей загрузке.			
Сетевой порт					
Модуль политики					
Домен процесса					

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.

🕈 Ад	министрирован	ие SELinux	_   :
<u>⊅</u> айл <u>С</u> правка			
Выбор:		¢.	â <u>A</u>
Статус	Bacctow		
Переключатель	BUCCTAH	лемпе произв	ольный влокирование
Присвоение меток файлам	Фильтр		
Сопоставление пользователей	+ to to tp	L	
Пользователь SELinux	Active	Module 🗸	Description
Сетевой порт		abrt	Allow ABRT to run in abrt_handle_event_
Модуль политики		abrt	Allow ABRT to modify public files used fo
Домен процесса		apache	Allow httpd to access cifs file systems
	✓	apache	Allow Apache to communicate with avan
		apache	Allow apache scripts to write to public co
		apache	Allow httpd to read home directories
		apache	Allow Apache to run in stickshift mode, r
		apache	Allow Apache to use mod_auth_pam
		apache	Allow Apache to query NS records
	✓	apache	Allow httpd cgi support
		apache	Allow httpd to run gpg in gpg-web domai
		apache	Allow HTTPD scripts and modules to con
		apache	Allow httpd to act as a relay
	<		>

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).

Изм.	Лист	№ докум	Подп	Дата

60



🕅 SELinu	ıx Boolean Lockdown 📃 🗆 🗙
<u>Ф</u> айл <u>С</u> правка	
Выбор:	Boolean: allow_httpd_sys_script_anon_write
Begin .	Allow apacha scripts to write to public content. Directories/
▽ abrt	Files must be labeled public rw content t.
abrt_handle_event	
abrt_anon_write	
Finish	
▽ apache	
httpd_enable_homedirs	
allow_httpd_sys_script_anon_write	
httpd_ssi_exec	
allow_httpd_anon_write	
httpd_can_check_spam	
httpd_dbus_avahi	
httpd_can_network_relay	🔄 🔿 🛑 Enable 💿 🛑 Disable 🛛 🕤 Default
· · · · · · · · · · · · · · · · · · ·	Выход Предыдущая Вперёд

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.

Изм.	Лист	№ докум	Подп	Дата

Добавить Свойства Уда Фильтр Определение файлов	лить Произвольный SELinux Тип Файла	
файлов	<ul> <li>Тип Файла</li> </ul>	_
1		
/.* /[^/]+ /afs /a?quota\.(user group)	root_t:s0 default_t:s0 etc_runtime_t:s0 mnt_t:s0 quota_db_t:s0	
/\.autorelabel /bin /bin/.*	etc_runtime_t.so etc_runtime_t:so bin_t:so bin_t:so	
/bin/alsaunmute /bin/bash /bin/bash2 /bin/d?ash	alsa_exec_t:s0 shell_exec_t:s0 shell_exec_t:s0 shell_exec_t:s0	-
	/[^/]+ /afs /a?quota\.(user group) /.autofsck /.autorelabel /bin /bin/.* /bin/alsaunmute /bin/bash /bin/bash2 /bin/d?ash	/[^/]+     etc_runtime_t:s0       /afs     mnt_t:s0       /a?quota\.(user group)     quota_db_t:s0       /.autofsck     etc_runtime_t:s0       /.autorelabel     etc_runtime_t:s0       /bin     bin_t:s0       /bin/.*     bin_t:s0       /bin/alsaunmute     alsa_exec_t:s0       /bin/bash     shell_exec_t:s0       /bin/drash     shell_exec_t:s0

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\_и 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.

Изм.	Лист	№ докум	Подп	Дата

SELinux-пользователь user\_u:

SELinux-пользователь user\_u напоминает обычного непривилегированного orpaниченного (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.

Изм.	Лист	№ докум	Подп	Дата



🕅 Админис	трировани	e SELinux		_ 0	×
<u>Ф</u> айл <u>С</u> правка					
Файл Справка           Выбор:           Статус           Переключатель           Присвоение меток файлам           Сопоставление пользователей           Пользователь SELinux           Сетевой порт           Модуль политики           Домен процесса	Добавить Фильтр ( Логин Имя default root system_u user	Свойства       Уд         SELinux       Пользователь         unconfined_u       unconfined_u         system_u       unconfined_u	алить Диапазон MLS/MCS s0-s0:c0.c1023 s0-s0:c0.c1023 s0-s0:c0.c1023 s0-s0:c0.c1023		
	(<		ш		~

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 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 pаботает в домене безопасности unconfined\_t через роль unconfined\_r, которой он сопоставлен.

Изм.	Лист	№ докум	Подп	Дата



ыбор:				
Статус				
Переключатель	дооавить сво	иства удалить		
Присвоение меток файлам	Фильтр			
Сопоставление пользователей	SELinux	Диапазон	Donu CELinux	-
Пользователь SELinux	Пользователь	MLS/MCS	POIN SELINUX	
Сетевой порт	git_shell_u		git_shell_r	
Модуль политики	guest_u	s0	guest_r	
Домен процесса	root	s0-s0:c0.c1023	staff_r sysadm_r system_r ur	IC
	staff_u	s0-s0:c0.c1023	staff_r sysadm_r system_r ur	nc
	sysadm_u	s0-s0:c0.c1023	sysadm_r	
	system_u	s0-s0:c0.c1023	system_r unconfined_r	
	unconfined_u	s0-s0:c0.c1023	system_r unconfined_r	
	user_u	s0	user_r	
	xguest_u	s0	xguest_r	
				C
	<	III	1	>

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).

🕅 Админи	стрирование SELinux			_ 0 ×
<u>Ф</u> айл <u>С</u> правка				
<b>Выбор:</b> Статус Переключатель	다. Добавить Свойства א	Эдалить	<b>Г</b> руппы	~
Присвоение меток файлам Сопоставление пользователей Пользователь SELinux	Фильтр SELinux Порт Тип	Иротокол	MLS/MCS Уровень	Порт
Сетевой порт	afs_bos_port_t	udp	s0	7007
Модуль политики	afs_client_port_t	udp	s0	7001
Домен процесса	afs_fs_port_t	udp	s0	7000
	afs_fs_port_t	tcp	s0	2040
	afs_fs_port_t	udp	s0	7005
	afs_ka_port_t	udp	s0	7004
	afs_pt_port_t	udp	s0	7002
	afs_vl_port_t	udp	s0	7003
	agentx_port_t	udp	s0	705
	agentx_port_t	tcp	s0	705
	amanda_port_t	udp	s0	10080-100
	amanda_port_t	tcp	s0	10080-100
	amavisd recy port t	tcn	50	10024
		111		>

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

Изм.	Лист	№ докум	Подп	Дата

66

ЦАУВ.14001-01 91 01

🕅 Аді	министрирование SELinux			_ 🗆 X
<u>Ф</u> айл <u>С</u> правка				
Выбор:	LB	0	-	
Статус		Vacauti		~
Переключатель	дооавить своиства	удалить	СПИСОК	
Присвоение меток файлам	Фильтр			
Сопоставление пользователей	SEL INUX DODT			<u></u>
Пользователь SELinux	Тип	<ul> <li>Протокол</li> </ul>	Порт	=
Сетевой порт	afs_bos_port_t	udp	7007	
Модуль политики	afs_client_port_t	udp	7001	
Домен процесса	afs_fs_port_t	tcp	2040	
	afs_fs_port_t	udp	7000, 7005	
	afs_ka_port_t	udp	7004	
	afs_pt_port_t	udp	7002	
	afs_vl_port_t	udp	7003	
	agentx_port_t	tcp	705	
	agentx_port_t	udp	705	
	amanda_port_t	tcp	10080-10083	
	amanda_port_t	udp	10080-10082	
4	amavisd_recv_port_t	tcp	10024	
5	amavisd send nort t	ten	10025	

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).

🔯 Адм	инистрирование SELinux	_ = ×
<u>Ф</u> айл <u>С</u> правка		
Фаил _ справка Выбор: Статус Переключатель Присвоение меток файлам Сопоставление пользователей Пользователь SELinux Сетевой порт Модуль политики Домен процесса	Создать Добавить Удалить       Включит         Фильтр	ъ аудит
		>

Рисунок 85 - Окно приложения "Администрирование SELinux"

вкладка "Модуль политики"

Изм.	Лист	№ докум	Подп	Дата

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.

🖹 Администрирование SELinux _ 🗆 🗙				
<u>Ф</u> айл <u>С</u> правка				
Файл Справка Выбор: Статус Переключатель Присвоение меток файлам Сопоставление пользователей Пользователь SELinux Сетевой порт Модуль политики	Разрешающий     Строгий       Фильтр			
Домен процесса	abrt_helper abrt_helper abrt_retrace_coredump abrt_retrace_worker accountsd acct ada admin_passwd afs afs_bosserver afs_fsserver			

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.

Изм.	Лист	№ докум	Подп	Дата

Файл sudoers должен редактироваться только командой visudo, которая блокирует файл и осуществит проверку грамматики. Это обязательно во избежание возникновения ошибок в cuнтаксисе 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.
- Ноst Alias (Псевдоним рабочей станции). Определяет, каким рабочим станциям присваиваются права.
- Соттапа 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 ("BCE"), и он может означать "BCE" пользователи, "BCE" 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

Изм.	Лист	№ докум	Подп	Дата

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 гооt 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

Изм.	Лист	№ докум	Подп	Дата

Чтобы дать пользователю права на выполнение от гооt 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 гооt 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

Изм.	Лист	№ докум	Подп	Дата

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

Изм.	Лист	№ докум	Подп	Дата

### 4.8 Библиотеки РАМ

МСВСфера 6.3 APM 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.

РАМ 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 РАМ, 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. РАМ 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 РАМ возвращает значение "success" (успех) или "failure" (неудача).

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

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

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

Изм.	Лист	№ докум	Подп	Дата
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.

2		system-auth (/etc/pam.d) - gedit	_ 0 ×
<u>Ф</u> айл <u>П</u> рав	ка <u>В</u> ид П <u>о</u> иск	к С <u>е</u> рвис <u>Д</u> окументы <u>С</u> правка	
🤷 🛅 От	крыть 🗸 🖄	Сохранить 📋 🍐 🥱 Отменить ⊘ 🔛 🐘 🏥 🍂	
📄 system-au	uth ≍		
#%PAM-1.0	-		_
# This file	e is auto-gener	rated.	
# User chan	nges will be de	estroyed the next time authconfig is run.	
auth	required	pam_env.so	
auth	sufficient	pam_fprintd.so	
auth	sufficient	pam_unix.so nullok try_first_pass	
auth	requisite	pam_succeed_if.so uid >= 500 quiet	
auth	required	pam_deny.so	
account	required	pam unix.so	=
account	sufficient	pam localuser.so	
account	sufficient	pam_succeed_if.so_uid < 500 quiet	
account	required	pam_permit.so	
nassword	requisite	nam cracklib so try first pass retry=3 type=	
password	sufficient	nam unix so sha512 shadow nullok trv first nass use authtok	
password	required	pam_deny.so	
passaora	required	poin_derif i so	
session	optional	pam lastlog.so	
	15. 17. 19.		
l	+1		
	Ť	Текст 🗸 Ширина табуляции: 8 🗸 Стр 21, Стлб 1	BCL

Рисунок 87 - Редактирование файла system-auth

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

🗵 user3@localhost:/var/log	_ = ×
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка	
[root@localhost log]# su user3 Последний вход в систему:Втр Янв 28 23:42:51 MSK 2014на pts/4 [user3@localhost log]\$ su Пароль: Пароль:	2
последний вход в систему:втр янв 28 23:43:13 MSK 2014на pts/4 [root@localhost log]#	



Изм.	Лист	№ докум	Подп	Дата

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

🗉 user3@localhost:/home/u	ser/Рабочий стол _ 🗆 🗙	ł
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> пра	вка	
[root@localhost Рабочий стол]# lastlog		^
Пользователь Порт С	Последний раз	
root pts/4	Втр Янв 28 23:43:13 +0400 2014	
bin	**Никогда не входил в систему**	
daemon	**Никогда не входил в систему**	
adm	**Никогда не входил в систему**	=
lp	**Никогда не входил в систему**	
sync	**Никогда не входил в систему**	
shutdown	**Никогда не входил в систему**	
halt	**Никогда не входил в систему**	
mail	**Никогда не входил в систему**	
uucp	**Никогда не входил в систему**	
operator	**Никогда не входил в систему**	
games	**Никогда не входил в систему**	
gopher	**Никогда не входил в систему**	
ftp	**Никогда не входил в систему**	

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:

Изм.	Лист	№ докум	Подп	Дата

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.

Σ	user2@l	ocalhost:/home/user3/Рабочий стол _ 🗆 🗙
<u>Ф</u> айл <u>П</u> рав	ка <u>В</u> ид П <u>о</u> исн	<u>Т</u> ерминал <u>С</u> правка
GNU nano 2	2.0.9	Файл: /etc/pam.d/system-auth
#%PAM-1.0 # This file # User chanc	is auto-gener	ated.
auth	required	pam_env.so
#auth #auth #auth	sufficient requisite required	pam_unix.so nullok try_first_pass pam_succeed_if.so uid >= 500 quiet pam_deny.so
auth auth account	required required required	pam_unix.so nullok try_first_pass pam_tally2.so deny=2 onerr=fail unlock_time=60 pam_tally2.so
account account account account	required sufficient sufficient required	pam_unix.so pam_localuser.so pam_succeed_if.so uid < 500 quiet pam_permit.so
password password password	requisite sufficient required	pam_cracklib.so try_first_pass retry=3 type= pam_unix.so sha512 shadow nullok try_first_pass use_a\$ pam_deny.so I
session session session session session	optional optional required [success=1 de required	pam_lastlog.so pam_keyinit.so revoke pam_limits.so fault=ignore] pam_succeed_if.so service in crond quiet\$ pam_unix.so
^G Помощь ^Х Выход	^О Записать ^Ј Выровнять	[Записано 28 строк] ^R ЧитФайл ^Y ПредСтр ^K Вырезать ^C ТекПозиц ^W Поиск ^V СледСтр ^U ОтмВырезк ^T Словарь ∵

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.

Изм.	Лист	№ докум	Подп	Дата

🗉 user3@localhost:~/Рабочий стол	-		×
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка			
[user@localhost Рабочий стол]\$ su user3 Пароль: su: неправильный пароль [user@localhost Рабочий стол]\$ su user3 Пароль: su: неправильный пароль [user@localhost Рабочий стол]\$ su user3 Пароль: Учетная запись заблокирована как следствие неудачных попыток входа (всего su: неправильный пароль [user@localhost Рабочий стол]\$ [user@localhost Рабочий стол]\$ [user@localhost Рабочий стол]\$ su user3 Пароль:		3)	
Последний вход в систему:Срд Янв 29 00:58:58 MSK 2014на pts/7 [user3@localhost Рабочий стол]\$			11

Рисунок 91 - Результат временной блокировки учетной записи пользователя

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

Σ					use	r3@localhost:/	home/user	3/Рабочий	стол		_ 0 ×
Φ	айл	Правка	<u>В</u> ид	П <u>о</u> иск	<u>Т</u> ерминал	<u>С</u> правка					
(	iNU I	nano 2.0	. 9			Файл: /var/	log/secure				
Jar	29	00:48:10	9 loca	lhost	su: pam_ta]	lly2(su:auth):	user user	2 (503) ta	lly 5, deny 2		
Jar	29	00:48:19	9 loca	lhost	su: pam_ta	lly2(su:auth):	user user	2 (503) ta	lly 6, deny 2		
Jar	29	00:48:3	l loca	lhost	su: pam_ta	lly2(su:auth):	user user	2 (503) ta	lly 7, deny 2		
Jar	29	00:48:50	9 loca	lhost	userhelper	[8838]: pam_tir	nestamp(sy	stem-confi	g-users:session):	updated timesta	amp file \$
Jar	29	00:48:50	9 loca	lhost	userhelper	[8845]: running	g '/usr/sh	are/system	-config-users/syst	em-config-users	s ' with \$
Jar	29	00:49:12	2 loca	lhost	su: pam_ta	lly2(su:auth):	user user	2 (503) ta	lly 8, deny 2		
Jar	29	00:49:5	7 loca	lhost	su: pam_un:	Lx(su:session)	: session	opened for	user user2 by use	r3(uid=504)	
Jar	29	00:50:3	5 loca	lhost	unix_chkpwd	[8914]: passwo	ord check	failed for	user (user)		22
Jar	29	00:50:3	5 loca	lhost	su: pam_uni	ix(su:auth): a	uthenticat	ion failur	e; logname=user3 u	id=503 euid=0 1	tty=pts/5\$
Jar	29	00:50:40	9 loca	lhost	unix_chkpwc	[8917]: passwo	ord check	failed for	user (user)		
Jar	29	00:50:40	9 loca	lhost	su: pam_un:	ix(su:auth): a	uthenticat	ion failur	e; logname=user3 u	id=503 euid=0 1	tty=pts/5\$
Jar	29	00:50:45	5 loca	lhost	unix_chkpwg	[8920]: passwo	ord check	failed for	user (user)		
Jar	29	00:50:45	5 loca	lhost	su: pam_un:	Lx(su:auth): a	uthenticat	ion failur	e; logname=user3 u	id=503 euid=0 1	tty=pts/5\$
Jar	29	00:50:45	5 loca	lhost	su: pam_ta	lly2(su:auth):	user user	(501) tal	ly 3, deny 2		=
Jar	29	00:51:3	7 loca	lhost	su: pam_ta	lly2(su:auth):	user user	(501) tal	ly 4, deny 2		
Jar	29	00:51:40	5 loca	lhost	su: pam_ta	lly2(su:auth):	user user	(501) tal	Ly 5, deny 2	1.1001 10	
Jar	29	00:52:18	3 loca	lhost	su: pam_un:	Lx(su:session)	: session	opened for	user user by user.	3(uid=503)	
Jar	29	00:56:43	3 loca	lhost	unix_chkpwd	[9025]: passwo	ord check	failed for	user (user3)		
Jar	29	00:56:43	3 loca	lhost	su: pam_uni	Lx(su:auth): a	uthenticat	ion failur	e; logname=user3 u	id=501 euid=0 1	tty=pts/5\$
Jar	29	00:56:4	7 loca	lhost	su: pam_un:	Lx(su:auth): a	uthenticat	ion failur	e; logname=user3 u	Ld=501 euid=0 1	tty=pts/5\$
Jar	29	00:56:5	l loca	lhost	su: pam_un:	Lx(su:auth): a	uthenticat	ion failur	e; logname=user3 u	1d=501 euid=0 1	tty=pts/5\$
Jar	29	00:56:5	l loca	lhost	su: pam_ta	lly2(su:auth):	user user	3 (504) ta	lly 3, deny 2		
Jar	29	00:57:30	5 loca	lhost	su: pam_un:	Lx(su:session)	: session	opened for	user root by user	B(uid=504)	
Jar	29	00:58:58	s loca	lnost	su: pam_un:	LX(SU:Session)	: session	opened for	user user3 by use	r3(u1d=504)	
Jar	29	00:59:0	/ Loca	lhost	su: pam_un:	LX(SU:Session)	: session	opened for	user user3 by use	r3(uid=501)	
Jar	29	01:07:30	9 loca	lhost	gnome-scree	ensaver-dialog	: gkr-pam:	unlocked	'login' keyring		
^G	Пом	ОЩЬ	^0	Запис	ать	R ЧитФайл	^Υ Πpe	дСтр	^К Вырезать	^С ТекПозиц	
^x	Вых	од	^J	Выров	нять	W Поиск	^V Сле	дСтр	^U ОтмВырезк	^Т Словарь	~

Рисунок 92 - Отчет о попытках аутентификации

Чтобы просмотреть заблокированных пользователей администратору с правами root, нужно ввести команду pam\_tally2 (рис. 93).

[root@localhost	Рабочий	стол]# раг	n_tally2	
Login	Failures	; Latest fa	ailure	From
user3	3	01/29/14	00:56:51	pts/5
[root@localhost	Рабочий	стол]#		

Рисунок 93 - Отчет о заблокированных пользователях

Изм.	Лист	№ докум	Подп	Дата

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

E	user2@l	ocalhost:/home/user3/Рабочий стол _ 🗆 🗆
<u>Ф</u> айл <u>П</u> рав	ка <u>В</u> ид П <u>о</u> ис	к <u>Т</u> ерминал <u>С</u> правка
GNU nano	2.0.9	Файл: /etc/pam.d/system-auth
.DAM 1 0		
%PAM-1.⊍ + This filo	is auto-dener	hete
# User chan	nes will be de	stroved the next time authconfig is run.
auth	required	pam env.so
auth	sufficient	pam fprintd.so
#auth	sufficient	pam unix.so nullok try first pass
#auth	requisite	pam_succeed_if.so_uid >= 500_quiet
#auth	required	pam_deny.so
auth	required	pam_unix.so nullok try_first_pass
auth	required	pam_tally2.so_deny=2_onerr=rait
account	required	pam_tatty2.so
account	required	pam unix.so
account	sufficient	pam localuser.so
account	sufficient	pam_succeed_if.so uid < 500 quiet
account	required	pam_permit.so
		and an old the sector first same action D to as
password	requisite	pam_unix_so_sha512_shadow_pullok_try_first_pass_uso_af
password	required	pam_unix.so snasiz snauow nuclok cry_iiisc_pass use_as
T	required	pan_deny.se
session	optional	pam lastlog.so
session	optional	pam keyinit.so revoke
session	required	pam_limits.so
session	[success=1 de	fault=ignore] pam_succeed_if.so service in crond quiet\$
session	required	pam_unix.so
^G Помощь	^0 Записать	^R ЧитФайл ^Y ПредСтр ^K Вырезать ^C ТекПозиц
Х Выход	^ј Выровнять	№ Поиск № СледСтр № ОтмВырезк № Словарь

Рисунок 94 - Файл /etc/pam.d/system-auth без параметра unlock\_time

🗉 user2@localhost:/home/user3/Рабочий стол	-		×
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка			
[user2@localhost Рабочий стол]\$ su user			^
Пароль:			
luser2@localhost Paбoчий стол]\$ su user			
Пароль:			
su: неправильный пароль			
[user2@localhost Рабочий стол]\$ su user			
Пароль:			
Учетная запись заблокирована как следствие неудачных попыток входа (всего		3)	• =
su: неправильный пароль			
[user2@localhost Рабочий стол]\$			~

Рисунок 95 - Блокировка пользователя после неудачных попыток авторизации

Изм.	Лист	№ докум	Подп	Дата

Разблокировать пользователя можно с правами root с помощью команды pam\_tally2 -u <имя пользователя> -r, как на рис. 96.

🗵 user2@localhost:/home/user3/Рабочий стол	 ×
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка	
[root@localhost Рабочий стол]# pam tally2 -u user -r	^
Login Failures Latest failure From	
user 3 01/29/14 00:33:47 pts/5	
[root@localhost Рабочий стол]#	
[root@localhost Рабочий стол]# pam_tally2 -u user3 -r	
Login Failures Latest failure From	
user3 6 01/29/14 00:33:14 pts/5	
[root@localhost Рабочий стол]#	
[root@localhost Рабочий стол]# <u>p</u> am_tally2	=
[root@localhost Рабочий стол]#	$\sim$

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).

🔄 Параметры	хранителя экрана х
<u>Т</u> ема хранителя экрана:	
Пустой экран Случайным образом	
Космос	
Папка рисунков	
Плавающие ступни	
Пульсирующие ячейки	
Просмотр	
Считать компьютер простаивающим через:	5 минут 
🗹 <u>З</u> апускать хранитель экрана, когда комп	ьютер простаивает
☑ <u>Б</u> локировать экран, когда запущен храни	тель экрана
<u>С</u> правка	Управление питанием Закрыть

Рисунок 97 - Время бездействия, установленное по умолчанию

Изм.	Лист	№ докум	Подп	Дата

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.

	USET2 Uset2 Ha localhost.localdomain			
Пароль:	0.000	Dafaamaaaa	en	
переключить пользователя	ОТМЕНИТР	<u>Разолокировать</u>		

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 ceancy, но не получит доступ к данным без повторной аутентификации для разблокировки ceanca (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

Изм.	Лист	№ докум	Подп	Дата

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).

🗷 mc [root@localhost.localdomain]:/dev _	. 0	×
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка		
[root@localhost dev]# rfkill Usage: rfkill [options] command Options: version show version (0.3)		^
help event list		I
block { <idx>,all,wifi,bluetooth,uwb,wimax,wwan,gps} unblock {<idx>,all,wifi,bluetooth,uwb,wimax,wwan,gps} [root@localhost dev]#</idx></idx>		~

Рисунок 99 - Параметры команды rfkill

Изм.	Лист	№ докум	Подп	Дата

### 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).

	Настройка Kickstart 🗆 🗆
айл Справка	
Основные настройки	Метод установки Выполнить новую установку
Параметры загрузчика Информация о разделах	<ul> <li>Обновить существующую систему</li> </ul>
Настройка сети Аутентификация Настройка брандмауэра Настройка дисплея Выбор пакетов Сценарий до установки Сценарий после установки	Установочный носитель © CD-ROM © NFS © FTP © НТТР © 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.

Изм.	Лист	№ докум	Подп	Дата

Основные настройки	Тип установки
Метод установки	<ul> <li>Устанавливать новый начальный загрузчик</li> </ul>
Параметры загрузчика Информация о разделах Настройка сети Аутентификация Настройка брандмауэра Настройка дисплея Выбор пакетов Сценарий до установки Сценарий после установки	<ul> <li>Не устанавливать загрузчик</li> <li>Обновить установленный загрузчик</li> </ul> Параметры GRUB № Использовать пароль GRUB Пароль: Повторите пароль: Эашифровать пароль GRUB Параметры установки Эагрузчик в MBR Загрузчик в первом секторе загрузочного раздела Параметры ядра:

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.

Изм.	Лист	№ докум	Подп	Дата

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.

	issue	(/etc) - gedit	:		_ 0 X
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид Г	1 <u>о</u> иск С <u>е</u> рвис	<u>Д</u> окументы	<u>С</u> правка		
🤷 🔄 Открыть 🗸	실 Сохранить	• 🚔 🕤 🕤	Отменит	• @   🏑	
📄 issue  🗶					
MSVSphere ARM release Kernel \r on an \m System Security is er	e 6.3 nabled.				
	Текст 🛩 Ши	ирина табуляц	ии: 8 🗸	Стр 1, Стлб 1	BCT

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).

Изм.	Лист	№ докум	Подп	Дата



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;
- 1 вставка названия текущего терминала;
- т вставка идентификатора архитектуры системы, например, i686;
- n вставка имени узла, которым является машина, также известным как имя хоста;
- о вставка доменного имени машины;
- r вставка номера релиза ядра, например, 2.6.11.12;
- t вставка текущего времени;

и 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.

Изм.	Лист	№ докум	Подп	Дата

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 (Туре): 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

Изм.	Лист	№ докум	Подп	Дата

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 равными. Таким образом, объекту действительно метки 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.



MLS label = Level + Categories; For example, L = Secret: cat1, cat2, cat5

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),

Изм.	Лист	№ докум	Подп	Дата

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.

Изм.	Лист	№ докум	Подп	Дата



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

[root@localhost ~]# getenforce	
Enforcing	
[root@localhost ~]#	
[root@localhost ~]#	
[root@localhost ~]#	
[root@localhost ~]# sestatus	
SELinux status:	enabled
SELinuxfs mount:	/selinux
Current mode:	enforcing
Mode from config file:	enforcing
Policy version:	24
Policy from config file:	mls
[root@localhost ~]# _	

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

Изм.	Лист	№ докум	Подп	Дата

ЦАУВ.14001-01 91 01

[mont@looslboot ~]	# opinfo			
TLOOCGIOCGINOSC 1	# SCINIU			
Statistics for nol	icu file:	/etc/selinux/mls	/nolicu/n	olicu.24
Policy Version & T	upe: v.24	(binary, mls)	· F=3. F	
2	21	2-		
Classes:	81	Permissions:	235	
Sensitivities:	16	Categories:	1024	
Types:	3049	Attributes:	263	
Users:	8	Roles:	14	
Booleans:	172	Cond. Expr.:	209	
Allow:	236253	Neverallow:	0	
Auditallow:	2	Dontaudit:	182022	
Type_trans:	7255	Type_change:	39	
Type_member:	68	Role allow:	29	
Role_trans:	107	Range_trans:	2483	
Constraints:	249	Validatetrans:	17	
Initial SIDs:	27	Fs_use:	22	
Genfscon:	81	Portcon:	426	
Netifcon:	1	Nodecon:	0	
Permissives:	0	Polcap:	2	
[root@localhost ~]	#			

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):

[root@localhost ~]	# seinfo /	/etc/selinux/targ	eted∕poli	cy∕policy.24
Statistics for pol Policy Version & 7	icy file: Ype: v.24	/etc/selinux/tar (binary, mls)	geted∕pol	icy∕policy.24
Classes:	81	Permissions:	235	
Sensitivities:	1	Categories:	1024	
Types:	3508	Attributes:	277	
Users:	9	Roles:	12	
Booleans:	190	Cond. Expr.:	225	
Allow:	275808	Neverallow:	0	
Auditallow:	97	Dontaudit:	202156	
Type_trans:	24055	Type_change:	38	
Type_member:	48	Role allow:	20	
Role_trans:	292	Range_trans:	3996	
Constraints:	87	Validatetrans:	0	
Initial SIDs:	27	Fs_use:	22	
Genfscon:	81	Portcon:	426	
Netifcon:	0	Nodecon:	0	
Permissives:	60	Polcap:	2	
[root0localhost ~]	#			

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 (puc. 111).

Изм.	Лист	№ докум	Подп	Дата





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).

2	user@localhost:~/Рабочий стол			
<u>Ф</u> айл	<u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка			
[user@ unconf [user@	localhost Рабочий стол]\$ id -Z ined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 localhost Рабочий стол]\$			

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.

Изм.	Лист	№ докум	Подп	Дата

ЦАУВ.14001-01 91 01

localhost login: user Password:	
[user@localhost~]\$	
Euser@localhost ~1\$	
[user@localhost ~]\$ echo "test" >> testfile	
[user@localhost ~1\$ ls -Z	
-rw-rw-r user user user_u:object_r:user_home_t:s0	testfile

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.

Изм.	Лист	№ докум	Подп	Дата

### 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;

Изм.	Лист	№ докум	Подп	Дата

- утилита load\_policy;
- утилита restorecon;
- утилита restorecond;
- утилита semodule;
- утилита setenforce;
- утилита setfiles;
- утилита AIDE;
- утилита АМТU;
- 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 "-1", 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.

-М — 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.

Изм.	Лист	№ докум	Подп	Дата

-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.

-Е — 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 -М.

#### 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).

Изм.	Лист	№ докум	Подп	Дата

Суперпользователь может менять любые данные любой учётной записи. Кроме того, только суперпользователь может использовать параметр -о 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.

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

-г, --гоот – меняет номер комнаты пользователя.

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

-и, --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

Изм.	Лист	№ докум	Подп	Дата

## 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]: т

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:

-с, --соттепт - 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.

Изм.	Лист	№ докум	Подп	Дата

-е, --ехріredate — 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.

-К, --key — используется для изменения значений по умолчанию, хранимых в файле /etc/login.defs (UID\_MIN, UID\_MAX, UMASK, PASS\_MAX\_DAYS и других).

Пример: -К 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 -К несколько раз, например: -К UID\_MIN=100 -K, UID\_MAX=499.

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

-р, --раssword — 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

Изм.	Лист	№ докум	Подп	Дата

### 5.6 Утилита usermod

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

Команда usermod поддерживает следующий набор опций:

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

-с, --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.

-е, --ехріredate — 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".

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

-р, --рassword — задать новый шифрованный пароль для учетной записи.

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

-и, --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

Изм.	Лист	№ докум	Подп	Дата

### 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.

Изм.	Лист	№ докум	Подп	Дата

-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.

-К — изменить значения по умолчанию (GID\_MIN, GID\_MAX и другие), которые хранятся в файле /etc/login.defs. Можно указать несколько параметров "-К".

Пример: -K GID\_MIN=100 -K GID\_MAX=499

-о — 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;

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

-р, --раssword - 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

Изм.	Лист	№ докум	Подп	Дата

### 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.

-1 — 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:
```

значения контекста;

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

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

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

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

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

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

--help – показать справку и выйти;

Изм.	Лист	№ докум	Подп	Дата

--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;

-Р – 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:

-о – компиляция является опциональной;

-b – проверка двоичных политик на корректность и допустимость;

-М – проверка политики MLS;

-d – вызывается режим отладки.

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

checkpolicy -b

Изм.	Лист	№ докум	Подп	Дата

### **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:

-і – игнорировать несуществующие файлы;

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

-е – 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;

-о – 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).

Изм.	Лист	№ докум	Подп	Дата

[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;

Изм.	Лист	№ докум	Подп	Дата

-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 -1 показать список установленных модулей (рис.

120).

[root@localhost		Рабочий	стол]#	semodule	-1
abrt	1.2.0				
accounts	sd	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	1.8.1			
asterisk	¢.	1.7.1			
audioent	ropy	1.6.0			
automour	nt	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

Изм.	Лист	№ докум	Подп	Дата

#### **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:

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

-d – показать, какая спецификация соответствует каждому файлу

-1 – отразить изменения меток в syslog.

-n – не менять метки файлов.

-q – подавить вывод, не относящийся к ошибкам

-r – использовать альтернативный путь к корневой директории

-е 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).

-о 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

Изм.	Лист	№ докум	Подп	Дата

### 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 АМТИ

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

АМТИ 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.

АМТU 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.

АМТИ 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.

Изм.	Лист	№ докум	Подп	Дата

Для проверки дисковых контроллеров (только IDE и SCSI) АМТU 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.

АМТU 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 АМТИ поддерживает следующий набор опций:

- -d Вывод сообщения об отладке;
- -т Выполнение теста памяти;
- -ѕ Выполнение теста разделения памяти;
- -і Запуск контроллера ввода/вывода тестирования диска;
- -п Запуск контроллера ввода/вывода проверки сети;
- -р 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

Изм.	Лист	№ докум	Подп	Дата
### 5.22 Утилита sudo

Утилита sudo предоставляет привилегии гооt 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.

-1 — 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 какойлибо 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.

-К — 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.

-р — 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.

-с — 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

Изм.	Лист	№ докум	Подп	Дата

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".

-а — 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 РАТН, 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 РАТН находится на машине, которая в настоящий момент не доступна.

Изм.	Лист	№ докум	Подп	Дата

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:

-а, --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.

Изм.	Лист	№ докум	Подп	Дата

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 'Ӌ' 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:

- -т модифицировать правило acl;
- -М просмотр acl записи для редактирования из файла;
- -b удаляет все acl правила;
- -к удаляет правила "по умолчанию";
- -s заменяет правила acl заданными;
- -d устанавливает правила по умолчанию;
- -R выполняет применение acl рекурсивно;
- -х удаляет указанное acl правило;
- -X просмотр acl записи для удаления из файла;
- -n отсутствие маски для эффективных прав;
- -L логический переход по символьным ссылкам;
- -Р 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.

Изм.	Лист	№ докум	Подп	Дата

### 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]# <u>h</u>wclock --localtime --systohc

Рисунок 126 – Установка времени

### 5.26 Утилита гпапо

Редактор гпапо 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;

Изм.	Лист	№ докум	Подп	Дата

### 114

#### ЦАУВ.14001-01 91 01

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

-С <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;

-К, --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;

-Т <#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;

-с, --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;

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

-р, --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;

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

Изм.	Лист	№ докум	Подп	Дата

### 115

#### ЦАУВ.14001-01 91 01

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

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

-х, --nohelp- не показывать две строки помощи внизу;

-z, --suspend – разрешить приостановку;

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

-а, -b, -e,-f, -g, -j, (игнорируется для совместимости с Рісо).

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).

Изм.	Лист	№ докум	Подп	Дата

116

Σ			root@loo	alhos	t:~/Рабочий стол	_ C	ı x
<u>Ф</u> айл	<u>П</u> равка	<u>В</u> ид Г	П <u>о</u> иск <u>Т</u> ерм	инал	<u>С</u> правка		
GNU	nano 2.0	.9		Новый	буфер	Изменен	
I want	to crea	te a ne	w file and	name	it testfile		
I							
							=
Имя Фа	йла для	записи:	testfile	8		 	
^G Пом	ОЩЬ						
^C 0TM	ена						~

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.

Изм.	Лист	№ докум	Подп	Дата

Зыбор:				
Статус				
Переключатель	дооавить свои	ства удалить		
Присвоение меток файлам	Фильтр			_
Сопоставление пользователей	SELinux	Лиапазон		~
Пользователь SELinux	Пользователь	MLS/MCS	Роли SELinux	
Сетевой порт	git_shell_u	s0	git_shell_r	
Модуль политики	guest_u	s0	guest_r	1
Домен процесса	root	s0-s0:c0.c1023	staff_r sysadm_r system_r un	c
	staff_u	s0-s0:c0.c1023	staff_r sysadm_r system_r un	c
	sysadm_u	s0-s0:c0.c1023	sysadm_r	
	system_u	s0-s0:c0.c1023	system_r unconfined_r	=
	unconfined_u	s0-s0:c0.c1023	system_r unconfined_r	
	user_u	s0	user_r	
	xguest_u	s0	xguest_r	
				Ŀ

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).

📸 sudoers (/etc) - gedit _ 🗆 >
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск С <u>е</u> рвис <u>Д</u> окументы <u>С</u> правка
📔 🔤 Открыть 🗸 🖄 Сохранить   📇   🕤 Отменить 💩   😹 📳 🗸
📄 sudoers 💥
<pre>## Next comes the main part: which users can run what software on ## which machines (the sudoers file can be shared between multiple ## systems). ## Syntax: ##</pre>
## user MACHINE=COMMANDS ##
## The COMMANDS section may have other options added to it.
## Allow root to run any commands anywhere root ALL=(ALL) ALL
<pre>## Allows members of the 'sys' group to run networking, software, ## service management apps and more. # %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS</pre>
<pre>## Allows people in group wheel to run all commands # %wheel ALL=(ALL) ALL</pre>
## Same thing without a password # %wheel ALL=(ALL) NOPASSWD: ALL
<pre>## Allows members of the users group to mount and unmount the ## cdrom as root # %users_ALL=/sbin/mount /mnt/cdrom. /sbin/umount /mnt/cdrom</pre>
<pre>## Allows members of the users group to shutdown this system # %users localhost=/sbin/shutdown -h now</pre>
<pre>## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment) #includedir /etc/sudoers.d</pre>
Текст 🗸 Ширина табуляции: 8 🗸 Стр 1, Стлб 1 ВСТ

Рисунок 130 – Конфигурационный файл /etc/sudoers

Изм.	Лист	№ докум	Подп	Дата

#### 118

#### ЦАУВ.14001-01 91 01

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 "%".

Изм.	Лист	№ докум	Подп	Дата

# 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.

Файл Плавка Спл	PKP			
<u>Ф</u> аилі <u>п</u> равка <u>С</u> пра	abka			
<b>R</b>	<b>4</b>	-		
Добавить пользоват	еля Добавить групп	у Свойства	Удалить Обновить Справка	
		Фильтр <u>п</u> оиска	: Применить с	рильтр
<u>П</u> ользователи <u>Г</u> руп	пы			
Имя пользователя	ID пользователя 🗸	Осн. группа	Полное имя	Of
root	0	root	root	/bi
bin	1	bin	bin	/sb
daemon	2	daemon	daemon	/sb
adm	3	adm	adm	/sb
lp	4	lp	lp	/sb
sync	5	root	sync	/bi
shutdown	6	root	shutdown	/sb
halt	7	root	halt	/sb
mail	8	mail	mail	/sb
uucp	10	uucp	uucp	/sb
operator	11	root	operator	/sb
games	12	users	games	/sb
gopher	13	gopher	gopher	/sb
ftp	14	ftp	FTP User	/sb
oprofile	16	oprofile	Special user account to be used by OProfile	/sb

Рисунок 131 – Вкладка пользователи менеджера пользователей

2		Менеджер пользователей 🛛 🗕 🗆 🛪
<u>Ф</u> айл <u>П</u> равка	<u>С</u> правка	
Добавить поль	зователя Доба	авить группу Свойства Удалить Обновить Справка
		Фильтр поиска: Применить фильтр
<u>П</u> ользователи	<u>Г</u> руппы	
Имя группы	ID группы ∽	Члены группы
root	0	halt, operator, root, shutdown, sync
bin	1	bin, daemon
daemon	2	bin, daemon
sys	3	adm, bin
adm	4	adm, daemon
tty	5	
disk	6	amandabackup
Ip	7	daemon, Ip
mem	8	
kmem	9	
wheel	10	
cdrom	11	
mail	12	mail, postfix
uucp	14	uucp
man	15	
oprofile	16	anrafila

Рисунок 132 – Вкладка группы менеджера пользователей

Изм.	Лист	№ докум	Подп	Дата

### 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

📸 auditd.conf (/etc/audit) - gedit	- 🗆
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск С <u>е</u> рвис <u>Д</u> окументы <u>С</u> правка	
🤷 🚍 Открыть 🗸 🌺 Сохранить 📄 🍰 Отменить 💩 🕌	`
📄 auditd.conf  🗶	
# # This file controls the configuration of the audit daemon #	
<pre>log_file = /var/log/audit/audit.log log_format = RAM  log_group = root priority_boost = 4 flush = INCREMENTAL freq = 20 num_logs = 5 disp_qos = lossy dispatcher = /sbin/audispd name_format = NONE ##name = mydomain max_log_file = 6 max_log_file_action = ROTATE space_left = 75 space_left = 75 space_left = cont admin_space_left = 50 admin_space_left = 50 admin_space_left = 50 disk_full_action = SUSPEND disk_full_action = SUSPEND disk_error_action = SUSPEND ##tcp_listen_port = tcp_listen_queue = 5 tcp_max_per_addr = 1 ##tcp_client_ports = 1024-65535 tcp_client_max_idle = 0 enable_krb5 = no krb5_orincipal = auditd</pre>	
<pre>krbs_principat = auditd ##krb5_key_file = /etc/audit/audit.key</pre>	
Текст 🗸 Ширина табуляции: 8 🗸 Стр 6, Стлб 17 В	ст

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

Изм.	Лист	№ докум	Подп	Дата

# 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.

0				н	астр	ойка	а дат	ы/времени _ 🗆	×
Дат	аи <u>в</u> р	емя	<u>ч</u> ас	овой	і поя	с			
Тек	ущие	дата	аивр	ремя	: Cp,	ц 27	Ноя	2013 21:54:10	
	С <u>и</u> нхр	ониз	зация	я дат	ыи	врем	ени п	ю сети	
Ус	танов	ка с	исте	мной	і дат	ыив	време	ни вручную:	
	<u>ц</u> ата							Время	
	< H	оябр	ь >			< 20	)13 >	<u>Ч</u> асы : 21 🗘	
8	Пнд	Втр	Срд	Чтв	Птн	Сбт	Вск	Минуты : 53 🗘	
	28	29	30	31	1	2	з		
	4	5	6	7	8	9	10	секунды. 50 🗸	
	11	12	13	14	15	10	1/		
	25	26	20	21	22	20	24		
	23	20	27	20	23	7	8		
			-						
									_
Спр	равка							Отменить ОК	

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.

Изм.	Лист	№ докум	Подп	Дата

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).

🍞 auditd.co	onf (/etc/audit) - gedit _ 🗆 🛛 🛪
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск С <u>е</u> рвис <u>Д</u> окуме	енты <u>С</u> правка
🤷 🔄 Открыть 🗸 🎂 Сохранить 📋	🕤 Отменить 💩 😹 🖫 🖺 🏘 🍂
📄 auditd.conf  🗶	
<pre># # This file controls the configuration of #</pre>	the audit daemon
<pre>log_file = /var/log/audit/audit.log log_format = RAW log_group = root priority_boost = 4 flush = INCREMENTAL freq = 20 num_logs = 5 disp_qos = lossy dispatcher = /sbin/audispd name_format = NONE ##name = mydomain max_log_file = 6 max_log_file = 6 max_log_file = 6 max_log_file_action = ROTATE space_left = 75 space_left = 75 space_left = 50 admin_space_left = 50 admin_space_left = 50 admin_space_left = 50 admin_space_left = 50 admin_space_left = 0 disk_error_action = SUSPEND disk_error_action = SUSPEND disk_error_action = SUSPEND disk_error_action = SUSPEND ##tcp_listen_port = tcp_listen_port = 1024-65535 tcp_client_max_idle = 0 enable_krbS = no krbS_principal = auditd ##krbS_key_file = /etc/audit/audit.key</pre>	
	Текст 🗸 Ширина табуляции: 8 🗸 Стр 16, Стлб 1 ВСТ

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

Изм.	Лист	№ докум	Подп	Дата

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

Изм.	Лист	№ докум	Подп	Дата

— 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
- -с, --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

Изм.	Лист	№ докум	Подп	Дата

- 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
- -х, --executable. Отчет об исполняемых объектах.

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

Изм.	Лист	№ докум	Подп	Дата

Image: state of the state o	
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка	
[root@localhost ~]# aureport	
Summary Report	
Range of time in logs: 15.08.2013 19:57:33.067 - 15.08.2013 21:16:00.524	
Selected time for report: 15.08.2013 19:57:33 - 15.08.2013 21:16:00.524	
Number of changes in configuration: 9	
Number of changes to accounts, groups, or roles: 0	
Number of logins: 2	
Number of failed logins: 0	
Number of authentications: 2	
Number of Talled authentications: 0	
Number of users: 3	
Number of best pamer. 1	
Number of executables: 26	
Number of files: 1097	
Number of AVC's: 1	
Number of MAC events: 2	
Number of failed syscalls: 4260	
Number of anomaly events: 0	
Number of responses to anomaly events: 0	
Number of crypto events: 0	
Number of keys: 0	
Number of process IDS: 69	
NUMBER OT EVENTS: 10530	

Рисунок 139 – Суммарный отчет

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

Σ.			root@lo	calhost:~/Рабочий стол _	x
<u>Φ</u> a	йл <u>П</u> равка	<u>В</u> ид П <u>о</u> и	іск <u>Т</u> ер	минал <u>С</u> правка	
26.	13.01.2014	10:06:30	root ?	? /usr/sbin/userhelper yes 719	2
27.	13.01.2014	10:06:55	root ?	:2 /usr/libexec/gdm-session-worker yes 729	
28.	13.01.2014	10:07:08	root ?	? /usr/sbin/userhelper yes 739	
29.	13.01.2014	10:38:34	root ?	? /usr/sbin/userhelper yes 830	
30.	13.01.2014	10:43:00	root ?	? /usr/sbin/userhelper yes 852	
31.	13.01.2014	11:58:58	Ivan ?	:2 /usr/libexec/gdm-session-worker yes 1090	
32.	13.01.2014	11:59:07	? ? :2	/usr/libexec/gdm-session-worker no 1101	
33.	13.01.2014	11:59:16	root ?	:2 /usr/libexec/gdm-session-worker yes 1105	
34.	13.01.2014	12:58:04	root ?	? /usr/sbin/userhelper yes 1304	
35.	13.01.2014	13:53:03	root ?	:2 /usr/libexec/gdm-session-worker no 1483	
36.	13.01.2014	13:53:14	root ?	:2 /usr/libexec/gdm-session-worker no 1487	
37.	13.01.2014	13:53:27	root ?	:2 /usr/libexec/gdm-session-worker no 1491	
38.	13.01.2014	13:53:38	? ? :2	/usr/libexec/gdm-session-worker no 1493	
39.	13.01.2014	13:53:52	root ?	:2 /usr/libexec/gdm-session-worker yes 1500	
40.	13.01.2014	13:54:17	root ?	? /usr/sbin/userhelper yes 1510 🛽	
41.	13.01.2014	13:58:32	root ?	:0 /usr/libexec/gdm-session-worker no 117	
42.	13.01.2014	13:59:23	root ?	:0 /usr/libexec/gdm-session-worker yes 124	
43.	13.01.2014	13:59:37	root ?	? /usr/sbin/userhelper yes 141	
44.	13.01.2014	14:11:35	root ?	? /usr/sbin/userhelper yes 198	-
45.	13.01.2014	16:04:58	root ?	:0 /usr/libexec/gdm-session-worker yes 117	
46.	13.01.2014	16:51:24	Ivan ?	:1 /usr/libexec/gdm-session-worker no 319	
47.	13.01.2014	16:51:37	root ?	:1 /usr/libexec/gdm-session-worker no 326	
48.	13.01.2014	16:51:51	root ?	:1 /usr/libexec/gdm-session-worker yes 330	

Рисунок 140 – Отчет о всех попытках аутентификации

Изм.	Лист	№ докум	Подп	Дата

### 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:

- -а, --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;
- с, --сотт сотт-пате. Искать события с заданным сотт пате (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;

Изм.	Лист	№ докум	Подп	Дата

- -m, --message message-type | сотта-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;
- -о, --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 по(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;

Изм.	Лист	№ докум	Подп	Дата

- 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;
- -х, --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.

E					root@l	oca	alhost:~						_ 0	×
<u>Φ</u> ай	іл	<u>П</u> равка	<u>В</u> ид	П <u>о</u> иск	<u>Т</u> ерминал	<u>C</u>	правка							
295 cred ss'	ses ac	=42949) ct="ro	67295 ot" ex	subj=sy e="/usr,	stem_u:syst /sbin/crond	tem d"	n_r:crond hostname	_t:s0- =? add	s0:c0. r=? te	c1023 rmina	msg=' l=cror	op=P/	AM:set =succe	< .
time type _r:c ses=	->T =L0 ron 8	hu Aug GIN ms d_t:s0	15 20 g=audi -s0:c0	:40:01 : t(13765 .c1023	2013 84801.511:3 old auid=42	391 294	106): pid 1967295 n	=27712 ew aui	uid=0 d=0 ol	subj: d ses:	=syste =42949	em_u: 967295	system 5 new	n
time type =8 s root	->T =US ubj " e	hu Aug ER_STAI =syster xe="/u:	15 20 RT msg m_u:sy sr/sbi	:40:01 =audit( stem_r: n/crond	2013 1376584801. crond_t:s0- " hostname=	.54 -s0 =?	45:39107) ):c0.c102 addr=? t	: user 3 msg= ermina	pid=2 op=PA l=cron	7712 M:ses res=	uid=0 sion_c succes	auid= open a ss'	=0 ses acct='	5
time type 8 su exe=	->T =CR bj= "/u	hu Aug ED_DIS system sr/sbi	15 20 P msg= _u:sys n/cron	:40:01 : audit(1: tem_r:c d" host	2013 376584801.6 rond_t:s0-s name=? addr	659 s0: r=?	9:39108): c0.c1023 ? termina	user msg=' l=cron	pid=27 op=PAM res=s	712 u setc: ucces	id=0 a red ac s'	auid=( cct="	0 ses= root"	=
time type sub oot" [roo	->T =US j=s ex t@l	hu Aug ER_END ystem_u e="/us ocalho:	15 20 msg=a u:syst r/sbin st ~]#	:40:01 : udit(13 :em_r:cro /crond"	2013 76584801.65 ond_t:s0-s0 hostname=7	59: 0:c ? a	39109): c0.c1023 addr=? te	user p msg='o rminal	id=277 p=PAM: =cron	12 ui sessi res=s	d=0 au on_clo uccess	uid=0 ose ao S'	ses=8 cct="r	3

Рисунок 141 – События журнала аудита

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

Изм.	Лист	№ докум	Подп	Дата



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

Изм.	Лист	№ докум	Подп	Дата

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;
- е [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;
- -і. Игнорировать ошибки при чтении правил из файла;
- - 1. Вывести список всех правил по одному правилу в строке;
- к ключ. Установить на правило ключ фильтрации. Ключ фильтрации это произвольная текстовая строка длиной не больше 31 символа. Ключ помогает

Изм.	Лист	№ докум	Подп	Дата

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

- текст. Послать в систему аудита пользовательское сообщение. Это возможно только из учетной записи root;
- р [rlwlxla]. Установить фильтр прав доступа для точки наблюдения. r=чтение, w=запись, x=исполнение, a=изменение атрибута;
- -г 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;
- -а список, действие. Добавить правило с указанным действием к концу списка;
- -А 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 вызоваlall]. 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

Изм.	Лист	№ докум	Подп	Дата

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;

Изм.	Лист	№ докум	Подп	Дата

 - -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).

Аді	инистрирование SELinu	ĸ		
<u>Ф</u> айл <u>С</u> правка				
Выбор:		_	A	
Статус			Durana ana	
Переключатель	создать дооавите	удалить	включить аудит	
Присвоение меток файлам	Фильтр			
Сопоставление пользователей	Имя модуля 🗸 В	ерсия		
Пользователь SELINUX	abrt 1	.2.0		
Сетевои порт	accountsd 1	.0.0		
Модуль политики	ada 1	.4.0		
Домен процесса	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		
				(

Рисунок 143 – Администрирование SELinux вкладка «Модуль политики»

Изм.	Лист	№ докум	Подп	Дата

### 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).

🗖 пример1 Properties	×
General Filter Columns Date Filter Expression	
Tab	
<u>N</u> ame: пример1	
Порядок событий Sort by:	
Order: ○ in Ascending ● i↓ Descending	
<u>П</u> рименить О <u>т</u> менить	<u>о</u> к

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).

General Filter Columns Date Filter Expression         uid = root         Удалить         Фобавить	пример1 Properties	×
uid = root Удалить С	General Filter Columns Date Filter Expression	
Добавить	uid = root	<u>У</u> далить
		Добавить

Рисунок 145 – Использование фильтра

Изм.	Лист	№ докум	Подп	Дата

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).

				пример1	Properties	5		×
1	General	Filter	Columns	Date Filter	Expression			
	Event Other	date fields					К <u>в</u> ерху Кни <u>з</u> у Удалить	
						~	Добавить	
				Пр	именить	О <u>т</u> менить	<u>о</u> к	

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).

	Audit Viewer					• •
<u>W</u> indow <u>L</u> ist <u>V</u> iew <u>H</u> elp						
пример1 отчет1						
						_
Filter: uid = root, date >= 13.01.2014 00:00:00.000					Search	4
Date   Other Fields						
13.01.2014 17: type=AVC, seresult=denied, seperms=rlimitinh	. pid=9891. com	m=anome-a	lock-app. scontext=syste	em u:sv	vstem r:system dbusd	Ξ
13.01.2014 17; type=USER_END, pid=9875, uid=root, auid=roo					op=PAM:session close	
13.01.2014 17: type=CRED DISP, pid=9875, uid=root, auid=ro		Even	t Details	×	, op=PAM:setcred, acct=	
13.01.2014 17: type=AVC, seresult=denied, seperms=search,	Identificatio	n			, scontext=system_u:sy	
13.01.2014 17: type=AVC, seresult=denied, seperms=search,	Time:	13.01.20	14 17:25:02		, scontext=system_u:sy	
13.01.2014 17: type=USER_START, pid=9875, uid=root, auid=r	Serial number	21. 550			3, op=PAM:session_ope	
13.01.2014 17: type=LOGIN, pid=9875, uid=root, subj=system	Records	-			ses=unset, ses=36	
13.01.2014 17: type=CRED_ACQ, pid=9875, uid=root, auid=un	USER_END	Field	Value		1023, op=PAM:setcred, a	
13.01.2014 17: type=USER_ACCT, pid=9875, uid=root, auid=u	(	acct	root		:1023, op=PAM:accounti	
13.01.2014 17: type=AVC, seresult=denied, seperms=write, pi		addr	?		=655363, scontext=sys	
13.01.2014 17: type=AVC, seresult=denied, seperms=write, pi		auid	root		=655363, scontext=sys	
13.01.2014 17: type=AVC, seresult=denied, seperms=rlimitinh		exe	/usr/sbin/crond	= 3	stem_r:system_dbusd_t:	
13.01.2014 17: type=AVC, seresult=denied, seperms=rlimitinh		nostname	/		/stem_r:system_dbusd_	
13.01.2014 17: type=USER_END, pid=9820, uid=root, auid=root		op	PAM:session_close		op=PAM:session_close	
13.01.2014 17: type=CRED_DISP, pid=9820, uid=root, auid=ro		pia	9875		, op=PAM:setcred, acct=	
13.01.2014 17: type=AVC, seresult=denied, seperms=write, pi		res	success		=655363, scontext=sys	
13.01.2014 17: type=AVC, seresult=denied, seperms=write, pi		ses	sustem unsustem merer	- 7	>=655363, scontext=sys	
13.01.2014 17: type=AVC, seresult=denied, seperms=search, p		torminal	system_u.system_r.cron		, scontext=system_u:sy	
13.01.2014 17: type=AVC, seresult=denied, seperms=search, p		terminal	cion	⋰,	, scontext=system_u:sy	
13.01.2014 17: type=USER_END, pid=9819, uid=root, auid=root		<u> </u>			op=PAM:session_close	
13.01.2014 17: type=CRED_DISP, pid=9819, uid=root, auid=ro	Previous Eve	ent <u>N</u> ex	kt Event <u>З</u> акрыть		, op=PAM:setcred, acct=	
13.01.2014 17: type=AVC, seresult=denied, seperms=rlimitinh					stem_r:system_dbusd_t:	
13.01.2014 17: type=AVC, seresult=denied, seperms=getattr, p	pid=9823, comm	=sa1, path=	=/root, dev=dm-0, ino=13	1073, s	scontext=system_u:syst	~

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).

Window Report View Helpпример1отчет1Ivangdmhaldaemonroot13.01.2014 09:12:13.00000013.01.2014 09:12:26.3470013.01.2014 09:12:26.3710013.01.2014 09:12:26.3710013.01.2014 09:12:28.0230013.01.2014 09:12:28.1380013.01.2014 09:12:28.1710013.01.2014 09:12:28.1710013.01.2014 09:13:41.7800013.01.2014 09:13:41.8070013.01.2014 09:13:41.8070013.01.2014 09:13:41.8070013.01.2014 09:13:41.8070013.01.2014 09:13:41.8070013.01.2014 09:13:41.8070013.01.2014 09:13:20.20790013.01.2014 09:13:20.20790013.01.2014 09:25:02.0790013.01.20	Audit Viewer							
Пример1Отчет1Ivangdmhaldaemonroot13.01.2014 09:12:13.00000013.01.2014 09:12:13.00500013.01.2014 09:12:13.00500013.01.2014 09:12:26.34700013.01.2014 09:12:26.37100013.01.2014 09:12:28.04300113.01.2014 09:12:28.10200113.01.2014 09:12:28.10200113.01.2014 09:12:28.17100113.01.2014 09:12:28.17300113.01.2014 09:12:28.17400113.01.2014 09:12:28.17500113.01.2014 09:12:28.17600113.01.2014 09:13:41.78000113.01.2014 09:13:41.80700113.01.2014 09:13:41.80700113.01.2014 09:13:01.42900113.01.2014 09:13:01.42900113.01.2014 09:15:01.42900113.01.2014 09:25:02.07900113.01.2014 09:35:01.64900113.01.2014 09:35:01.64900113.01.2014 09:35:01.64900113.01.2014 09:35:01.64900113.01.2014 09:35:01.64900113.01.2014 09:40:01.83500113.01.2014 09:40:01.845001 <td><u>W</u>indow <u>R</u>eport <u>V</u>iew <u>H</u>e</td> <td>elp</td> <td></td> <td></td> <td></td> <td></td>	<u>W</u> indow <u>R</u> eport <u>V</u> iew <u>H</u> e	elp						
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 09:12:13.005         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 09:12:28.102         0         0         0         1           13.01.2014 09:12:28.171         0         0         1         1           13.01.2014 09:12:28.171         0         0         1         1           13.01.2014 09:13:41.807         0         0         1         1           13.01.2014 09:13:41.807         0         0         1         1           13.01.2014 09:14:20.517         0         0         1         1           13.01.2014 09:15:01.429         0         0         1         1           13.01.20	пример1 отчет1							
Ivangdmhaldaemonroot13.01.2014 09:12:13.000000113.01.2014 09:12:13.005000113.01.2014 09:12:6.347000113.01.2014 09:12:26.347000113.01.2014 09:12:28.043000113.01.2014 09:12:28.102000113.01.2014 09:12:28.138000113.01.2014 09:12:28.171000113.01.2014 09:12:28.171000113.01.2014 09:12:28.171000113.01.2014 09:12:28.171000113.01.2014 09:13:41.78000113.01.2014 09:13:41.80700113.01.2014 09:15:01.42900113.01.2014 09:15:01.42900113.01.2014 09:15:01.42900113.01.2014 09:15:01.42900113.01.2014 09:15:01.42900113.01.2014 09:25:02.07900113.01.2014 09:35:01.64900113.01.2014 09:35:01.64900113.01.2014 09:35:01.64900113.01.2014 09:35:01.64900113.01.2014 09:35:01.64900113.01.2014 09:35:01.64900113.01.2014 09:40:01.83500113.01.2014								
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 09:12:28.171       0       0       0       1         13.01.2014 09:12:28.171       0       0       0       1         13.01.2014 09:12:28.171       0       0       0       1         13.01.2014 09:12:28.171       0       0       0       1         13.01.2014 09:13:41.807       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 09:15:01.429       0       0       0       1         13.01.2014 09:20:01.618       0       0       1       1 <td< td=""><td></td><td>Ivan</td><td>gdm</td><td>haldaemon</td><td>root</td><td></td></td<>		Ivan	gdm	haldaemon	root			
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 09:12:28.171       0       0       0       1         13.01.2014 09:12:28.171       0       0       0       1         13.01.2014 09:12:28.171       0       0       0       1         13.01.2014 09:13:41.780       0       0       1       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 09:15:01.429       0       0       0       1         13.01.2014 09:20:01.618       0       0       1       1 <td< td=""><td>13.01.2014 09:12:13.000</td><td>0</td><td>0</td><td>0</td><td>1</td><td></td></td<>	13.01.2014 09:12:13.000	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 09:12:28.171       0       0       0       1         13.01.2014 09:12:28.171       0       0       0       1         13.01.2014 09:12:28.171       0       0       0       1         13.01.2014 09:12:28.171       0       0       0       1         13.01.2014 09:12:28.171       0       0       0       1         13.01.2014 09:13:41.807       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 09:15:01.429       0       0       0       1         13.01.2014 09:20:01.618       0       0       1       1         13.01.2014 09:30:01.250       0       0       1       1 <td< td=""><td>13.01.2014 09:12:13.005</td><td>0</td><td>0</td><td>0</td><td>1</td><td></td></td<>	13.01.2014 09:12:13.005	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 09:12:28.171       0       0       0       1         13.01.2014 09:12:28.171       0       0       0       1         13.01.2014 09:12:28.171       0       0       0       1         13.01.2014 09:13:41.07       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 09:15:01.429       0       0       0       1         13.01.2014 09:20:01.618       0       0       1       1         13.01.2014 09:30:01.250       0       0       1       1         13.01.2014 09:35:01.649       0       0       1       1	13.01.2014 09:12:18.001	0	0	0	1			
13.01.2014 09:12:26.371000113.01.2014 09:12:28.043000113.01.2014 09:12:28.102000113.01.2014 09:12:28.138000113.01.2014 09:12:28.171000113.01.2014 09:12:28.171000113.01.2014 09:12:28.171000113.01.2014 09:12:28.171000113.01.2014 09:13:41.78000113.01.2014 09:13:41.80700113.01.2014 09:14:20.51700113.01.2014 09:15:01.42900113.01.2014 09:20:01.61800113.01.2014 09:30:01.25000113.01.2014 09:35:01.64900113.01.2014 09:35:01.64900113.01.2014 09:40:01.83500113.01.2014 09:40:01.835001	13.01.2014 09:12:26.347	0	0	0	1			
13.01.2014 09:12:28.043000113.01.2014 09:12:28.102000113.01.2014 09:12:28.138000113.01.2014 09:12:28.171000113.01.2014 09:12:28.245000113.01.2014 09:13:41.78000113.01.2014 09:13:41.80700113.01.2014 09:13:41.80700113.01.2014 09:14:20.51700113.01.2014 09:15:01.42900113.01.2014 09:20:01.61800113.01.2014 09:35:01.64900113.01.2014 09:35:01.64900113.01.2014 09:40:01.83500113.01.2014 09:40:01.835001	13.01.2014 09:12:26.371	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 09:12:28.171       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 09:13:41.807       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 09:20:01.618       0       0       0       1         13.01.2014 09:20:01.618       0       0       1       1         13.01.2014 09:30:01.250       0       0       1       1         13.01.2014 09:35:01.649       0       0       1       1         13.01.2014 09:40:01.835       0       0       1       1 <td< td=""><td>13.01.2014 09:12:28.043</td><td>0</td><td>0</td><td>0</td><td>1</td><td></td></td<>	13.01.2014 09:12:28.043	0	0	0	1			
13.01.2014 09:12:28.138       0       0       1         13.01.2014 09:12:28.171       0       0       1         13.01.2014 09:12:28.245       0       0       1         13.01.2014 09:12:28.245       0       0       1         13.01.2014 09:13:41.780       0       0       1         13.01.2014 09:13:41.807       0       0       1         13.01.2014 09:13:41.807       0       0       1         13.01.2014 09:13:41.807       0       0       1         13.01.2014 09:13:41.807       0       0       1         13.01.2014 09:14:20.517       0       0       1         13.01.2014 09:15:01.429       0       0       1         13.01.2014 09:25:02.079       0       0       1         13.01.2014 09:30:01.250       0       0       1         13.01.2014 09:35:01.649       0       0       1         13.01.2014 09:35:01.649       0       0       1         13.01.2014 09:40:01.835       0       0       1         13.01.2014 09:40:01.835       0       0       1	13.01.2014 09:12:28.102	0	0	0	1			
13.01.2014 09:12:28.171       0       0       1         13.01.2014 09:12:28.245       0       0       0       1         13.01.2014 09:12:28.245       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       1       1         13.01.2014 09:30:01.250       0       0       1       1         13.01.2014 09:35:01.649       0       0       1       1         13.01.2014 09:35:01.649       0       0       1       1         13.01.2014 09:40:01.835       0       0       1       1         13.01.2014 09:40:01.835       0       0       1       1	13.01.2014 09:12:28.138	0	0	0	1			
13.01.2014 09:12:28.245       0       0       1         13.01.2014 09:13:41.780       0       0       1         13.01.2014 09:13:41.807       0       0       1         13.01.2014 09:13:41.807       0       0       1         13.01.2014 09:13:41.807       0       0       1         13.01.2014 09:14:20.517       0       0       1         13.01.2014 09:14:20.540       0       0       1         13.01.2014 09:15:01.429       0       0       1         13.01.2014 09:20:01.618       0       0       1         13.01.2014 09:30:01.250       0       0       1         13.01.2014 09:35:01.649       0       0       1         13.01.2014 09:35:01.649       0       0       1         13.01.2014 09:35:01.649       0       0       1         13.01.2014 09:35:01.649       0       0       1         13.01.2014 09:40:01.835       0       0       1	13.01.2014 09:12:28.171	0	0	0	1			
13.01.2014 09:13:41.780       0       0       1         13.01.2014 09:13:41.807       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 09:14:20.517       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       1       1         13.01.2014 09:30:01.250       0       0       1       1         13.01.2014 09:35:01.649       0       0       1       1         13.01.2014 09:35:01.649       0       0       1       1         13.01.2014 09:35:01.649       0       0       1       1         13.01.2014 09:40:01.835       0       0       1       1	13.01.2014 09:12:28.245	0	0	0	1			
13.01.2014 09:13:41.807       0       0       1         13.01.2014 09:14:20.517       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 09:14:20.540       0       0       0       1         13.01.2014 09:15:01.429       0       0       0       1         13.01.2014 09:20:01.618       0       0       1         13.01.2014 09:30:01.250       0       0       1         13.01.2014 09:35:01.649       0       0       1         13.01.2014 09:35:01.649       0       0       1         13.01.2014 09:35:01.649       0       0       1         13.01.2014 09:40:01.835       0       0       1	13.01.2014 09:13:41.780	0	0	0	1			
13.01.2014 09:14:20.517       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 09:15:01.429       0       0       0       1         13.01.2014 09:20:01.618       0       0       1         13.01.2014 09:30:01.250       0       0       1         13.01.2014 09:35:01.649       0       0       1         13.01.2014 09:35:01.649       0       0       1         13.01.2014 09:35:01.649       0       0       1         13.01.2014 09:35:01.649       0       0       1         13.01.2014 09:35:01.649       0       0       1	13.01.2014 09:13:41.807	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       1         13.01.2014 09:25:02.079       0       0       1         13.01.2014 09:30:01.250       0       0       1         13.01.2014 09:30:01.250       0       0       1         13.01.2014 09:30:01.250       0       0       1         13.01.2014 09:30:01.250       0       0       1         13.01.2014 09:30:01.250       0       0       1         13.01.2014 09:30:01.250       0       0       1         13.01.2014 09:30:01.250       0       0       1         13.01.2014 09:40:01.835       0       0       1	13.01.2014 09:14:20.517	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 09:30:01.250       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 09:14:20.540	0	0	0	1			
13.01.2014 09:20:01.618       0       0       1         13.01.2014 09:25:02.079       0       0       1         13.01.2014 09:30:01.250       0       0       1         13.01.2014 09:30:01.250       0       0       1         13.01.2014 09:35:01.649       0       0       1         13.01.2014 09:40:01.835       0       0       1	13.01.2014 09:15:01.429	0	0	0	1			
13.01.2014 09:25:02.079       0       0       0       µ         13.01.2014 09:30:01.250       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 09:20:01.618	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 09:25:02.079	0	0	0	h			
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 09:30:01 250	0	0	0	1			
13.01.2014 09:40:01.835 0 0 0 1 13.01.2014 09:40:01.835 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 09.40.01.835	0	0	0	1			

Рисунок 149 – Создание отчета

Изм.	Лист	№ докум	Подп	Дата

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

	Audit Event Sour	ce x
□ <u>I</u> nclude	rotated files	
Syster     Sys	n audit log	
<u>L</u> og file:	audit.log	•
⊖ <u>F</u> ile		
<u>P</u> ath:		Browse
Примени	о <u>т</u> менить	<u>о</u> к

Рисунок 150 – Выбор источника хранения событий

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

-	Export	×
<u>И</u> мя:	пример1	
Сохранить в <u>п</u> апке	la root	\$
▷ Просмотреть дру	/гие папки	
File type: CSV		\$
Automatic file type	e e <u>x</u> tension	
	Отменить Сох	ранить

Рисунок 151 – Экспорт документа

Сохранить полученные отчеты можно с помощью "Window"->"Save layout as" или "List"->"Save Configuration as".

Изм.	Лист	№ докум	Подп	Дата

### 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.

Изм.	Лист	№ докум	Подп	Дата

# 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;

Изм.	Лист	№ докум	Подп	Дата

- 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 APM 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.

Изм.	Лист	№ докум	Подп	Дата

### 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 гооt 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

Изм.	Лист	№ докум	Подп	Дата

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 Арасhe (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.

Изм.	Лист	№ докум	Подп	Дата
# 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@lo	ocalhost Рабочий	стол]# stat Пример.	.txt			
File:	«Пример.txt»					
Size:	Θ	Blocks: 0	IO Block: 4096	пустой	обычный	файл
Device:	fd00h/64768d	Inode: 943150	Links: 1			
Access:	(0644/-rw-rr-	-) Uid: ( 0/	root) Gid: (	0/	root)	
Access:	2013-12-13 11:10	5:34.690676970 +0400	Ð			
Modify:	2013-12-13 11:10	6:33.562579823 +0400	Ð			
Change:	2013-12-13 11:10	6:33.562579823 +0400	Ð			

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.

Изм.	Лист	№ докум	Подп	Дата

😥 📩 🚃 🌵 💻 🙁 24 °С Птн, 13 Дек, 11:27 🛛 го	ot
📧 root@localhost:~/Рабочий стол _ 🗆	×
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка	
[root@localhost Рабочий стол]# touch -а Пример.txt	^
[root@localhost Рабочий стол]# stat Пример.txt	
File: «Пример.txt»	
Size: 26 Blocks: 8 IO Block: 4096 обыч	
ный файл	
Device: fd00h/64768d Inode: 917617 Links: 1	
Access: (0644/-rw-rr) Uid: ( 0/ root) Gid: ( 0/	
root)	
Access: 2013-12-13 11:27:24.437454562 +0400	
Modify: 2013-12-13 11:19:36.336510988 +0400	
Change: 2013-12-13 11:27:23.416454485 +0400	

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.

	Ģ	) 📩 💼 🦉	<b>(</b> ) 📃	<mark>∂</mark> 24 °C	Птн, 13 Д	leк, 11:3	1 root
2	roo	t@localho	ost:~/Pa(	бочий ст	ол		_ 🗆 🗙
<u>Ф</u> айл	<u>П</u> равка <u>В</u> ид	П <u>о</u> иск	<u>Г</u> ерминал	п <u>С</u> прави	ка		
[root@ld	ocalhost Paб	очий стол	]# touch	h - т Прин	wep.txt		^
[root@ld	ocalhost Pa6	очий стол	]# stat	Пример.	txt		
File:	«Пример.txt	»					
Size:	26	Bloc	:ks: 8		IO Block:	4096	обычн
ый файл							
Device:	fd00h/64768	d Inod	le: 9176	17 I	Links: 1		
Access:	(0644/-rw-r	r) U	Jid: (	0/	root) G	id: (	0/
root)							
Access:	2013-12-13	11:31:13.	5926472	65 +0400			
Modify:	2013-12-13	11:31:12.	5695111	13 +0400			
Change:	2013-12-13	11:31:12.	5695111	13 +0400			

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.

	root@localhost:~/Рабочий стол	_ 0	×
<u>Ф</u> айл	<u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка		
[root@l [root@l File: Size: Device: Access: Access: Modify: Change:	ocalhost Рабочий стол]# touch -d "2015-10-20 13:13:13 " Пример ocalhost Рабочий стол]# stat Пример.txt «Пример.txt» 26 Blocks: 8 IO Block: 4096 обычный фа fd00h/64768d Inode: 917617 Links: 1 (0644/-rw-rr) Uid: ( 0/ root) Gid: ( 0/ root 2013-12-13 11:47:19.322700100 +0400 2015-10-20 13:13:13.0000000000 +0400 2013-12-13 11:47:18.302239646 +0400	.txt айл ot)	



Изм.	Лист	№ докум	Подп	Дата

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

📧 root@localhost:~/Рабочий стол _ 🗆								
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> пра	вка							
[root@localhost Рабочий стол]# touch Этало	н.txt							
[root@localhost Рабочий стол]# stat Эталон	.txt							
File: «Эталон.txt»								
Size: 0 Blocks: 0	IO Block: 4096	пустой обычный файл						
Device: fd00h/64768d Inode: 943151	Links: 1							
Access: (0644/-rw-rr) Uid: ( 0/	root) Gid: (	0/ root)						
Access: 2013-12-13 11:52:30.330481684 +040	Θ							
Modify: 2013-12-13 11:52:29.200498654 +040	Θ							
Change: 2013-12-13 11:52:29.200498654 +040	Θ							
[root@localhost Рабочий стол]#								
[root@localhost Рабочий стол]# touch Приме	p.txt -r Эталон.t	xt						
[root@localhost Рабочий стол]# stat Пример	.txt							
File: «Пример.txt»	21 21							
Size: 26 Blocks: 8	IO Block: 4096	обычный файл						
Device: fd00h/64768d Inode: 917617	Links: 1							
Access: (0644/-rw-rr) Uid: ( 0/	root) Gid: (	0/ root)						
Access: 2013-12-13 11:53:31.156485339 +040	Θ							
Modify: 2013-12-13 11:52:29.200498654 +040	Θ							
Change: 2013-12-13 11:53:30.132691416 +040	Θ							

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 АМТИ

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.

АМТU (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.

2	root@localhost:~/Рабочий стол	_ 0	×
<u>Ф</u> айл	<u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка		
[root@	localhost Рабочий стол]# amtu -h		^
Usage:	amtu [-dmsinph]		
d	Display debug messages		
m	Execute Memory Test		
s	Execute Memory Separation Test		
i	Execute I/O Controller - Disk Test		
n	Execute I/O Controller - Network Test		
р	Execute Supervisor Mode Instructions Test		
h	Display help message		
[root@	localhost Рабочий стол]#		
[root@	localhost Рабочий стол]#		
[root@	localhost Рабочий стол]#		
[root@	local∯ost Рабочий стол]# amtu -m		
Execut	ing Memory Test		
Memory	Test SUCCESS!		

Рисунок 158 – Пример выполнения команд АМТИ

Изм.	Лист	№ докум	Подп	Дата

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.

			roo	t@localhos	t:~/P	абочий	стол				_	×
<u>Ф</u> айл	<u>П</u> равк	а <u>В</u> ид	П <u>о</u> иск	<u>Т</u> ерминал	<u>С</u> пра	авка						
[root@]	localho	st Pa6	очий сто	ол]# rpm -\	/a							^
	т.	/usr/s	hare/pea	ar/.depdb								
	т.	/usr/s	hare/pea	ar/.depdblc	ock							
S.5	т.	/usr/s	hare/pea	ar/.filemap	D							
	т.	/usr/s	hare/pea	ar/.lock								
.M		/var/c	ache/li	bvirt/qemu								
S.5	т.	/usr/s	hare/tex	xmf/web2c/u	updma	p.cfg						
	т. с	/etc/s	sconfi	g/system-co	onfig	-users						
L.	с	/etc/p	am.d/fi	ngerprint-a	auth							
L.	с	/etc/p	am.d/pas	ssword-auth	n							
L.	с	/etc/p	am.d/sma	artcard-aut	th							
L.	c	/etc/p	am.d/sys	stem-auth								
S.5	т. с	/etc/s	ecurity,	/sepermit.c	conf							
S.5	т. с	/etc/g	gz.modu	les								
S.5	т. с	/etc/m	aven/mav	ven2-depmap	o.xml							
(	5	/usr/l	ib64/Pe	gasus/provi	iderMa	anagers/	/libCM	PIProv	iderMa	anager	. S0	
(	5	/usr/l	ib64/Pe	gasus/provi	iders,	/libComp	outers	SystemP	rovid	er.so		
(	5	/usr/l	ib64/Pe	gasus/provi	iders,	/lib0SPr	rovide	er.so				
(	5	/usr/l	ib64/Pe	gasus/provi	iders,	/libProd	cessPr	rovider	. SO			
(	5	/usr/l	ib64/Pe	gasus/provi	iders,	/libSLPF	Provid	der.so				
(	5	/usr/l	ib64/li	bCIMxmlIndi	icati	onHandle	er.so					-
(	5	/usr/l	ib64/li	bDefaultPro	ovide	rManager	r.so					_
(	5	/usr/l	ib64/li	bpegclient.	. SO							
(	j	/usr/l	ib64/li	bpegcommon.	. SO							~

Рисунок 159 - Проверка установленных пакетов на полноту

Изм.	Лист	№ докум	Подп	Дата

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 "с", 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;
- Т время модификации файла;
- D устройство;
- U пользователь;
- G группа;
- М 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.

Изм.	Лист	№ докум	Подп	Дата

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.

📧 root@localhost:/media/MSVSphere_6.3_Server/Packages _ 🗆 🗙
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка
<pre>[root@localhost Packages]# tcpdump tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes 15:29:00.005787 IP 10.0.2.15.mdns &gt; 224.0.0.251.mdns: 0 PTR (QM)? _pgpkey-hkpt cp.local. (40)</pre>
15:29:00.030166 IP 10.0.2.15.48212 > ns1.ptcomm.ru.domain: 35183+ PTR? 251.0.0.2
15:29:00.032985 IP ns1.ptcomm.ru.domain > 10.0.2.15.48212: 35183 NXDomain 0/1/0 (99)
15:29:00.033110 IP 10.0.2.15.32852 > ns1.ptcomm.ru.domain: 6712+ PTR? 15.2.0.10. in-addr.arpa. (40)
15:29:00.035531 IP ns1.ptcomm.ru.domain > 10.0.2.15.32852: 6712 NXDomain 0/1/0 ( 117)
15:29:00.035840 IP 10.0.2.15.40992 > ns1.ptcomm.ru.domain: 40861+ PTR? 35.32.234 .85.in-addr.arpa. (43)
15:29:00.038249 IP ns1.ptcomm.ru.domain > 10.0.2.15.40992: 40861* 1/2/2 PTR ns1. ptcomm.ru. (134)
15:29:05.029622 ARP, Request who-has 10.0.2.2 tell 10.0.2.15, length 28 15:29:05.029716 ARP, Reply 10.0.2.2 is-at 52:54:00:12:35:02 (oui Unknown), lengt h 46
15:29:05.029909 IP 10.0.2.15.60098 > ns1.ptcomm.ru.domain: 33842+ PTR? 2.2.0.10. in-addr.arpa. (39)
15:29:05.092206 IP ns1.ptcomm.ru.domain > 10.0.2.15.60098: 33842 NXDomain 0/1/0 (116)

Рисунок 160 - Вывод информации о сетевых пакетах

Изм.	Лист	№ докум	Подп	Дата

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;

-е - включает вывод данных канального уровня (например, МАС-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;

Изм.	Лист	№ докум	Подп	Дата

-р - 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.

Изм.	Лист	№ докум	Подп	Дата

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.

7	Wireshark: Cap	ture Interfaces				_ 0 ×
Device	Description	IP	Packets	Packets/s		Stop
🔊 eth0		fe80::a00:27ff:fefb:1296	0	0	Start	Options
🔊 virbr0		192.168.122.1	0	0	Start	Options
🗩 any	Pseudo-device that captures on all interfaces	unknown	0	0	Start	Options
🔊 usbmon1	USB bus number 1	unknown	224	0	Start	Options
🛃 lo		127.0.0.1	0	0	Start	Options
<u>С</u> правка	]					<u>З</u> акрыть

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 реар-пд 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).

Изм.	Лист	№ докум	Подп	Дата

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).

📶 Wireshark: Capture Op	tions _ 🗆 ×
Capture	
Interface: eth0	~
IP address: fe80::a00:27ff:fefb:1296	
Link-layer header type: Ethernet 💲	
Capture packets in promiscuous mode	
Capture packets in pcap-ng format (experimental)	
Limit each packet to 1 bytes	
Capture Filter:	<b>~</b>
Capture File(s)	Display Options
File: <u>B</u> rowse	☑ Update list of packets in real time
Use <u>m</u> ultiple files	
$\checkmark$ Next file every1 $\stackrel{\frown}{\searrow}$ megabyte(s)	Automatic scrolling in live capture
$\Box$ Next file every $1$ $\frac{\uparrow}{\lor}$ minute(s) $\diamondsuit$	✓ <u>H</u> ide capture info dialog
✓ Ring buffer with 2 ↓ files	
□ Stop capture after 1 🗍 🗍 file(s)	Name Resolution
-Stop Capture	✓ Enable <u>M</u> AC name resolution
🗆 after 🛛 1 🚔 packet(s)	Enable network name resolution
□ after 1	
□ after 1 🗇 minute(s)   ≎	$\checkmark$ Enable <u>transport</u> name resolution
Справка	О <u>т</u> менить <u>S</u> tart

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...".

Изм.	Лист	№ докум	Подп	Дата

### 155

### ЦАУВ.14001-01 91 01

7					Captu	ıring	fron	n eti	10 - 1	Wir	resh	ark						_ 0	×
<u>F</u> ile <u>E</u> d	it <u>V</u> iew	<u>G</u> 0	<u>C</u> ap	ture	<u>A</u> nalyz	e <u>S</u> t	atisti	cs .	Telep	hon	уI	ools	<u>H</u> elp						
<b>e</b> ( )		<u>e</u> i (	<b>)</b>		Ξ.	×	3	٢	ß	2	4	•	4		₹		J		~
Filter:											~	Expre	essior	Cl	ea <u>r</u>	App <u>ly</u>	y		
No	Time					Sou	rce					Dest	inatio	n			Protocol	Inf	0
40	3.0690	51				212	.30.	134.	167			10.0	.2.15	;			ТСР	[T(	0
41	3.0690	61				10.	0.2.	15				212.	30.13	34.167	7		TCP	435	5
42	3.0932	75				10.	0.2.	15				224.	0.0.2	251			MDNS	Sta	ar
43	3.1215	63				10.	0.2.	15				224.	0.0.2	251			MDNS	Sta	ar
44	3.2835	07				10.	0.2.	15				224.	0.0.2	22			IGMP	٧3	1
45	3.2836	85				Rea	ltek	U_12	:35:	02		Broa	dcast				ARP	Who	3
46	3.8198	28				10.	0.2.	15				224.	0.0.2	251			MDNS	Sta	ar
47	4.1928	83				212	.30.	134.	167			10.0	.2.15	<b>;</b>			тср	[T(	
48	4.1929	10				212	.30.	134.	167			10.0	.2.15	5			TCP	[T0	
49	4.1929	22				10.	0.2.	15				212.	30.13	34.167	/		ТСР	435	5
50	4.2040	57				212	.30.	134.	167			10.0	.2.15	5			ТСР	[TO	
51	4.2040	69				212	.30.	134.	167			10.0	.2.15	)	_		HTTP	HT	
52	4.2040	77				10.	0.2.	15				212.	30.13	34.167	/		тср	435	<b>)</b> [~
<				-	0													1	>
▷ Frame	1 (342	byte	s on	n wir	e, 342	byte	es ca	aptu	red)										
Ether	net II,	Src:	Cad	dmusC	o_tb:1	2:96	(08	:00:	27:11	):1	2:96	5), D:	st: B	roadc	ast	(††:	TT:TT:T	t:tt:	1~
<								- 111											>
0000 ff	ff ff	ff ft	fff	08 0	0 27	fb 12	2 96	08	00 4	51	Θ			·	.E.				1
0010 01	48 00	00 00	00	80 1	1 39	96 0	9 00	00	00 f	f f	f	.н		9					Ξ
0020 ff	ff 00	44 00	9 43	01 3	4 51	7e 0	1 01	06	00 f	3 b	f	D	.C.4	Q~					
0030 54	75 00	00 00	00	00 0	0 00	00 00	9 00	00	00 0	0 0	0	Tu							~
eth0: •	<live cap<="" td=""><td>oture i</td><td>n pro</td><td>gress</td><td>&gt; Fi</td><td>Pack</td><td>ets:</td><td>52 Di</td><td>splay</td><td>ed:</td><td>52  </td><td>Marke</td><td>d: 0</td><td>Profil</td><td>e: De</td><td>fault</td><td>:</td><td></td><td></td></live>	oture i	n pro	gress	> Fi	Pack	ets:	52 Di	splay	ed:	52	Marke	d: 0	Profil	e: De	fault	:		

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).

Изм.	Лист	№ докум	Подп	Дата

🔘 Приложения	Переход Система 🍪 🚳 🗾		🥼 🛃 C	рд, 12 Фев, 19:12 <b>гоот</b>
	Capturing from eth0	- Wireshark	Mark Packet (toggle) Set Time Reference (tog	igle)
	Elit View Go Capture Analyze Statistics fel	ephony <u>I</u> oois <u>H</u> eip	Apply as Filter Prepare a Filter	> >
Домашняя пап пользователя г	Filter.	Ethernet IP	Conversation Filter Colorize Conversation	>
	1356         243.059204         63.245.217.1           1357         243.059213         10.0.2.15	UDP PN-CBA Server	Follow TCP Stream	>
Корзина	1358         243.062319         63.245.217.1s           1359         243.062330         10.0.2.15           1360         245.831542         10.0.2.15	63.245.217 63.245.217	Follow SSL Stream	
	1361         245.831698         63.245.217.26           1362         246.056418         63.245.217.26           1363         246.056443         10.0.2.15	10.0.2.15 10.0.2.15 63.245.217	Decode As	
	1364         255.227909         10.0.2.15           1365         256.153286         10.0.2.15           1366         256.153495         212.188.7.123	224.0.0.25 212.188.7. 10.0.2.15	Show Packet in New Wir	ndow
	1367         256.169836         212.188.7.123           1368         256.169869         10.0.2.15	10.0.2.15 212.188.7.1	TCP h <sup>-</sup> 23 TCP 59	tti = 99( -
	▷ Frame 1366 (60 bytes on wire, 60 bytes capture ▷ Ethernet II, Src: RealtekU_12:35:02 (52:54:00)	ed) :12:35:02), Dst: Cad	musCo_fb:12:96 (08:00)	:27
	0000 08 00 27 fb 12 96 52 54 00 12 35 02 08 00 0010 00 28 02 ed 00 00 40 06 8f 9d d4 bc 07 7b	45 00'RT 0a 00 .(@	5E. {	
	0020 02 0f 00 50 ea 03 01 c5 64 ae 47 52 dc be 0030 ff ff 52 b6 00 00 00 00 00 00 00 00 O eth0: <live capture="" in="" progress=""> Fi Packets: 1368 Di</live>	50 10P d. R	GRP.	v

Рисунок 165 - Фильтрация пакетов

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

🗖 Cap	oturing from eth0 - Wi	reshark	>
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> na	lyze <u>S</u> tatistics Telephon	y <u>T</u> ools <u>H</u> elp	
	X 2 👌 🗚	<b>♦ ३ ∓ ±</b>	
Filter: ip.addr eq 212.188.7.123 and i	p.addr eq 10.0.2.15	← Expression Clea <u>r</u> A	pp <u>l</u> y
No Time	Source	Destination	Protocol Info
802 236.532383	10.0.2.15	212.188.7.123	TCP 599(
804 236.561278	10.0.2.15	212.188.7.123	HTTP GET
805 236.561490	212.188.7.123	10.0.2.15	TCP http
808 236.577685	212.188.7.123	10.0.2.15	HTTP HTTI
815 236.617464	10.0.2.15	212.188.7.123	TCP 599(
902 236.753887	10.0.2.15	212.188.7.123	HTTP GET
903 236.753956	212.188.7.123	10.0.2.15	TCP http
1053 237.009141	212.188.7.123	10.0.2.15	HTTP HTTI
1054 237.009154	10.0.2.15	212.188.7.123	TCP 599(
1365 256.153286	10.0.2.15	212.188.7.123	TCP 599(
1366 256.153495	212.188.7.123	10.0.2.15	TCP htt
1367 256.169836	212.188.7.123	10.0.2.15	TCP http
1368 256.169869	10.0.2.15	212.188.7.123	TCP 599(
<ul> <li>III</li> </ul>			>
Frame 1366 (60 bytes on wire.	60 bytes captured)		
Ethernet II, Src: RealtekU_12	:35:02 (52:54:00:12:3	5:02), Dst: CadmusCo_fb	:12:96 (08:00:27
< <u>&lt;</u>	Ш		>
0000 08 00 27 fb 12 96 52 54 (	0 12 35 02 08 00 45 0	0'RT5E.	
0010 00 28 02 ed 00 00 40 06 8	3f 9d d4 bc 07 7b 0a 0	0 .(@{	
0020 02 0f 00 50 ea 03 01 c5 0	54 ae 47 52 dc be 50 1	0P d.GRP.	
0030 ff ff 52 b6 00 00 00 00	00 00 00 00	R	
eth0: <live capture="" in="" progress=""> Fi.</live>	Packets: 1368 Displaye	ed: 61 Mark Profile: Defa	ault

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.

7	Wireshark: Find Packet	_ 0 ×			
Find					
By:	er 🔿 <u>H</u> ex value 🔿 <u>S</u> tring				
Filter:	F <u>i</u> lter:				
Search In	String Options	Direction			
O Packet list	🗋 Case sensitive	⊖ <u>U</u> р			
O Packet details	Character set:	● <u>D</u> own			
Packet bytes	ASCII Unicode & Non-Unicode				
<u>С</u> правка	О <u>т</u> менить	<u>Н</u> айти			

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.

🔘 Приложения Пе	ереход Система 🍪	۴ 🖄			ф 📃	Срд, 12 Ф	ев, 19:23	root
Компьютер	a Edit View Go Cor	Capt	uring from eth0 - Wiresha	rk	_	×		
	Open Open <u>R</u> ecent	Ctrl+O	× © 👌 🖻 +			~		
Домашняя папі пользователя к	<u>C</u> lose	Ctrl+W	Source	xpression Clear Ap	Protocol	Info ^		
Корзина	<u>S</u> ave Save <u>A</u> s Shi	Ctrl+S ft+Ctrl+S	10.0.2.15 6 63.245.217.105 1 10.0.2.15 6	3.245.217.105 0.0.2.15 3.245.217.105		355 http 355 345		
	File Set Export	> >	63.245.217.20 1 as "Plain <u>T</u> ext" file	0.0.2.15	ТСР	htti		
	<u>P</u> rint Ouit	Ctrl+P Ctrl+O	as "PostScript" file as "CSV" (Comma Separated as "C Arrays" (packet bytes)	Values packet summar file	y) file			
	1367 256.159836 1368 256.169869 1369 511.248305		as XML - "P <u>S</u> ML" (packet sun as XML - "P <u>D</u> ML" (packet det	nmary) file ails) file				
	Frame 26 (126 bytes Ethernet II, Src: Ca	on wire, dmusCo_fb	Selected Packet <u>Bytes</u> Objects			Ctrl+H	HTTP DICOM	
00 00 00 00	90         52         54         00         12         35         02           10         00         70         e7         39         40         60           20         86         a7         aa         35         00         50           30         39         08         67         37         00         00	08 00 27 40 06 ec 8c da ab 47 45 54	7 fb 12 96 08 00 45 00 F 7 9 0a 00 02 0f d4 1e 85 00 03 e8 02 50 18 4 20 2f 63 67 69 2d 62 9	T5 'E. p.9@.@y .5.PP. .g7GE T /cgi-b				
<u> </u>	eth0: <live capture="" in="" pro<="" th=""><th>gress&gt; Fi</th><th>Packets: 1369 Displayed: 13</th><th>69 Ma Profile: Defau</th><th>ult</th><th>,al</th><th></th><th></th></live>	gress> Fi	Packets: 1369 Displayed: 13	69 Ma Profile: Defau	ult	,al		

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).

V	Display filter: none	lausucs					_ 0 /
Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
▼ Frame	100,00 %	1370	605505	0,005	0	0	0,000
▼ Ethernet	100,00 %	1370	605505	0,005	0	0	0,00
	99,56 %	1364	605181	0,005	0	0	0,000
<ul> <li>User Datagram Protocol</li> </ul>	5,47 %	75	14760	0,000	0	0	0,00
Bootstrap Protocol	0,29 %	4	1864	0,000	4	1864	0,00
Domain Name Service	5,18 %	71	12896	0,000	71	12896	0,00
Internet Group Management Protocol	0,15 %	2	108	0,000	2	108	0,00
Iransmission Control Protocol	93,94 %	1287	590313	0,005	1250	571189	0,00
<ul> <li>Hypertext Transfer Protocol</li> </ul>	2,70 %	37	19124	0,000	19	7519	0,00
Line-based text data	0,73 %	10	7521	0,000	10	7521	0,00
Portable Network Graphics	0,36 %	5	3370	0,000	5	3370	0,00
Compuserve GIF	0,07 %	1	459	0,000	1	459	0,00
Media Type	0,15 %	2	255	0,000	2	255	0,00
Address Resolution Protocol	0,44 %	6	324	0,000	6	324	0,00
k							
<u>С</u> правка							<u>З</u> акрыт

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.

Изм.	Лист	№ докум	Подп	Дата

# 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;

Изм.	Лист	№ докум	Подп	Дата

- утилита ір;
- 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'/>
```

Изм.	Лист	№ докум	Подп	Дата

#### 161

### ЦАУВ.14001-01 91 01

```
</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.gcow2'/>
     <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

Изм.	Лист	№ докум	Подп	Дата

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, a 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

Изм.	Лист	№ докум	Подп	Дата

# 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:poль: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 -А добавляет новое правило в конец заданной цепочки, ключ -t указывает на используемую таблицу, ключ -о 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 -т загружает расширения, ключ --state проверяет признак состояния соединения. Примером

Изм.	Лист	№ докум	Подп	Дата

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
1	[root@localhost	~]#	iptables	-F
1	[root@localhost	~]#	iptables	-t nat -A POSTROUTING -o eth14 -j MASQUERADE
1	[root@localhost	~]#	iptables	-I FORWARD 1 -i tap0 -j ACCEPT
1	[root@localhost	~]#	iptables	-I FORWARD 1 -o tap0 -m statestate RELATED,ESTAB
I	LISHED -j ACCEPI	ſ		
	[root@localhost	~]#		

Рисунок 172 - Настройка iptables на host-системе

# 8.6 Утилита ір

Утилита ір позволяет выполнять настройку сетевой подсистемы.

Для выполнения какой-либо операции после команды ір 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).

	LrootWlocalhost "I# ip addr	
	1: lo: <loopback,up,lower_up> mtu 16436 qdisc noqueue state UNKNOWN</loopback,up,lower_up>	
	link/loopback 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</broadcast,multicast>	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</broadcast,multicast>	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</broadcast,multicast,up,lower_up>	state UNKNOW
- [	N	
	link/ether 52:54:00:d5:83:7f brd 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</broadcast,multicast>	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

Изм.	Лист	№ докум	Подп	Дата

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

Изм.	Лист	№ докум	Подп	Дата

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.

Флаг SELinux	Описание		
virt_use_comm	Разрешает использовать СОММ-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 РСІ-устройств		
virt_use_usb	Разрешает использование USB-устройств		
virt_use_xserver	Разрешает взаимодействие с X Window		
	System		

Таблица 2. Флаги SELinux для виртуализации

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.

Изм.	Лист	№ докум	Подп	Дата

vn	test_vm Виртуальная машина — ×
<u>Ф</u> айл Виртуальная <u>м</u> аши	на <u>В</u> ид Отправить комбинацию <u>к</u> лавиш
	<ul> <li>✓ [</li></ul>
<ul> <li>Overview</li> <li>Performance</li> <li>Processor</li> <li>Memory</li> <li>Boot Options</li> <li>VirtIO Disk 1</li> <li>IDE CDROM 1</li> <li>NIC :d5:2e:75</li> <li>Mышь</li> <li>Дисплей VNC</li> <li>Sound: ich6</li> <li>Serial 1</li> <li>Bидео</li> <li>Controller usb</li> <li>Controller IDE</li> </ul>	<ul> <li>Основные параметры         <u>Н</u>азвание: test_vm         UUID: 6а3faac5-6c93-8d03-a360-12b2b55b5221         Состояние: Выключена         Описание: <b>Подробнее о гипервизоре</b>         Гипервизор: kvm         Архитектура: x86_64         Эмулятор: /usr/libexec/qemu-kvm         <b>Operating System</b>             Xocr: unknown         Product name: unknown         <b>Архрісаtions Настройки мащины</b> </li> </ul>
	<ul> <li>Растроики нашины</li> <li>Безопасность</li> <li>Модель: selinux</li> <li>Тип: Одинамический ()</li> <li>Статический ()</li> <li>Статический ()</li> <li>Метка: system usystem risvirt tis0:c300.c686</li> </ul>
<u>До</u> бавить оборудование	Отмените Примените

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.

Изм.	Лист	№ докум	Подп	Дата

# 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.

Изм.	Лист	№ докум	Подп	Дата

# 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.

настройка Kickstart _ 🗆 🛪				
<u>Ф</u> айл Справка				
Основные настройки Метод установки Параметры загрузчика Информация о разделах Настройка сети Аутентификация Настройка брандмауэра Настройка дисплея Выбор пакетов	Настройка бранди SELinux: Уровень защиты: Доверенные слуу	мауэра Активно Включить брандмауэр жбы: УWWW (НТТР) FTP SSH Telnet	¢   ¢	
Сценарий до установки Сценарий после установки	Другие порты (10	Mail (SMTP)		

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

Изм.	Лист	№ докум	Подп	Дата

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.

Изм.	Лист	№ докум	Подп	Дата

Цепочки организованны в четыре таблицы:

- гаw 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 ceancobom ypobne (stateful firewall). Система позволяет определить, к какому соединению или ceancy принадлежит пакет. Механизм определения состояний анализирует все пакеты кроме тех, которые были помечены NOTRACK в таблице гаw.

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.

Изм.	Лист	№ докум	Подп	Дата

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.

Изм.	Лист	№ докум	Подп	Дата

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]

Изм.	Лист	№ докум	Подп	Дата

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] -Е цепочка новое\_название

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

iptables [-t таблица] -Р 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] - А 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).

Изм.	Лист	№ докум	Подп	Дата

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 паt "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, состояние NEW позволяет выделять только пакеты, 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.

Изм.	Лист	№ докум	Подп	Дата

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.

- [!] -р, --рготосоl 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 IPадресом (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

Изм.	Лист	№ докум	Подп	Дата

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;
- о, --оиt-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;
- с, --set-counters пакеты байты. Параметр позволяет при добавлении или изменении правил одновременно инициализировать счетчики числа пакетов и размера данных.

Изм.	Лист	№ докум	Подп	Дата

# **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 "-М" позволяет указать путь до программы modprobe. По умолчанию путь берется из файла /proc/sys/kernel/modprobe.

Ключ "-с" (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 "-с", 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 "-с" (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.

Изм.	Лист	№ докум	Подп	Дата

# **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 iptablessave, 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

Изм.	Лист	№ докум	Подп	Дата

АССЕРТ 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, --аррепd. 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 –1;
- -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;

Изм.	Лист	№ докум	Подп	Дата
- -N, --new-chain. Создает новую пользовательскую цепочку с заданным именем.
   Имя цепочки может содержать до 31 символа, число пользовательских цепочек не ограничено;
- -х, --delete-chain. Удаляет указанную пользовательскую цепочку. Удалить можно только те цепочки, которые не используются в качестве операции в какойлибо 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 --atomicfile или указывается в переменной окружения EBTABLES ATOMIC FILE;
- --аtomic-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 --аtomic-init или --аtomic-save. Файл, с которым работает данная команда, задается с помощью опции --аtomic-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.

Изм.	Лист	№ докум	Подп	Дата

### 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".

🚅 Mac	тер настройки межсетевого экрана 🛛 🗙 🗙
Ma	тер настройки межсетевого экрана
Информац	19
Мастер наст экрана для і	ройки поможет создать конфигурацию зашей системы.
Ответьте на вернетесь к неиспользуе	заданные мастером вопросы. Затем вы основному приложению, при этом все мые параметры будут спрятаны.
Настройки м	ожно будет изменить в меню Параметры.
О <u>т</u> ме	нить Назад <u>В</u> перёд <u>О</u> К

Рисунок 177 - Окно приветствия приложения "Мастер настройки межсетевого экрана"

Изм.	Лист	№ докум	Подп	Дата

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".

🚘 Мастер настройки межсетевого экрана 🛛 🗙
Мастер настройки межсетевого экрана
Основные настройки межсетевого экрана
Тип вашей системы?
Система с сетевым доступом
Система без сетевого доступа не нуждается в сетевом экране. Ее выбор отключит использование экрана. В противном случае выберите вариант Система с сетевым доступом.
О <u>т</u> менить На <u>з</u> ад <u>В</u> перёд <u>ОК</u>

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".

	Мастер настройки межсетевого экрана 🛛 🗙 🗙
	Мастер настройки межсетевого экрана
Уровен	ь пользователя
Укажите	е ваш опыт работы с межсетевым экраном.
Экспе	рт 🗘
Выберит межсете произво <i>Начинае</i>	ге <i>Эксперт</i> , если вы знакомы с настройками евого экрана или намереваетесь добавить льные правила. В противном случае выберите <i>ощий</i> .
0	<u>тменить</u> На <u>з</u> ад <u>В</u> перёд <u>О</u> К

Рисунок 179 - Окно выбора уровня работы с межсетевым экраном пользователя

Изм.	Лист	№ докум	Подп	Дата

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".

🛃 Mac	тер настройки меж	сетевого экрана 🛛 🗙
Mac	стер настройки м	ежсетевого экрана
Конфигура	ция	
Можно сохр конфигурац	анить конфигурацию ию.	или загрузить текущую
🗌 Оставит	ъ конфигурацию	
Загрузить	Рабочая станция	конфигурация
Если вы отм существуюц	Сервер цие настройки экрана	<i>конфигурацию</i> , то будут переопределены.
Отме	нить На <u>з</u> ад	<u>в</u> перёд <u>О</u> К

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;

Изм.	Лист	№ докум	Подп	Дата

– 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 РОРЗ 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.

Изм.	Лист	№ докум	Подп	Дата

186

		•	
Мастер Примен	нить Перезагрузить Включить	Выключить	
Доверенные службы	Здесь можно задать доверенные о	лужбы, которые будут доступны из лк	бых
Другие порты	сетей и узлов.		
Доверенные интерф	Служба	Помощник по системе С	onnti
Маскарад	🗌 Bacula		
Перенаправление по	DNS		
Фильтр ІСМР	FTP	ftp	
Пользовательские п	🗌 IMAP через SSL		
	IPsec		
	mDNS (Multicast DNS)		
	□ NFS4		
	OpenVPN		
	POP-3 yepes SSL		
	RADIUS		
	Red Hat Cluster Suite		
	<		>
	Разрешить доступ только к не	обхолимым службам	

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 IMAPдоступ 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.

🔘 Приложения	Переход Система 🍯	🤌 🖉				ų,	<b></b>	Птн, 7 с	Фев, 15:34	root
Компьютер	<b>.</b>	Настроі	іка межо	сетевого экј	рана		-	• ×		
	<u>Ф</u> айл <u>П</u> араметры <u>С</u>	правка								
命	🔐 I 🖉									
Домашняя пал	Мастер Примен	нить Перезагрузи	ить Вк	лючить Вь	ключить					
пользователя г	Парарации с спинби	-								
	Доверенные Служоы	Добавьте дополн быть доступны и	ительны з других	е порты или сетей или vз	диапазоны портов, влов.	которые	должны	4		
	Доверенные интерф	Порт 🗸 Проток	ол Слу	/жба			Добав	ить		
Корзина	Маскарад		<b>.</b>	Порт	и протокол	×	Manau			
	Перенаправление по		Выберит	ге запись из	списка или введите	порт и	измен	ИТБ		
	Фильтр ІСМР		протоко	л.			⊻дали	ить		
	пользовательские п		Порт 🗸	Протокол	Служба					
			1	tcp	tcpmux	=				
			1	udp	tcpmux					
			2	tcp	compressnet					
			2	tap	compressnet					
			5	udp	rie					
			7	tcp	echo	~				~
		A December -	🗆 Опре	деленный п	ользователем					
	Image: Market and M	л Разрешить д			отов:		ампор	TOB.		
	Межсетевой экран вкл	лючен.		_						
					Отменить	OK				
			_							
🗃 Настройка ме	ежсетевого									

Рисунок 182 - Добавление порта и протокола

Изм.	Лист	№ докум	Подп	Дата

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.

<b>.</b>	Настрой	ка межсетевого экрана	>
<u>Ф</u> айл <u>П</u> араметры <u>С</u>	правка		
🚅 🛛 🚽	' 🙈		
Мастер Примен	нить Перезагрузи	ть Включить Выключить	
Доверенные службы Другие порты	Отметьте интерф системе.	ейсы, которым нужно предоставить полный д	оступ к
Доверенные интерф	Интерфейс 🗸	Описание	Добавить
Иаскарад	□ マ eth+	Все устройства eth+	
Теренаправление по	eth0	wired Ethernet, HWADDR 08:00:27:FB:12:96	
Фильтр ІСМР	eth	Не настроен	
Тользовательские п	ippp+	Все устройства іррр+	
	isdn+	Все устройства isdn+	
	ppp+	Все устройства ppp+	-
	tun+	Все устройства tun+	
	wlan+	Все устройства wlan+	
< <u> </u>	Отметьте инт соответствую	ерфейсы, только если вы доверяете всем учас щей сети.	тникам в

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.

<b>.</b>	Настро	йка межсетевого экрана	×
<u>Ф</u> айл <u>П</u> араметры <u>С</u>	правка		
🚔 🎺 Мастер Примен	🥱 нить Перезагруз	ить Включить Выключить	
Доверенные службы Другие порты Доверенные интерф Маскарад	Возможность ма маршрутизатор, при этом не буде Отметить интер	скарада (только для IPv4) позволяет настроить уз подключающий локальную сеть к Интернету. Лок ет видна извне, будет лишь доступен один адрес. фейсы для маскарада.	ел или альная сеть
Перенаправление по	Интерфейс 🗸	Описание	Добавить
Фильтр ІСМР	□ マ eth+	Все устройства eth+	
Пользовательские п	eth0	wired Ethernet, HWADDR 08:00:27:FB:12:96	
	🗌 eth	Не настроен	
	ippp+	Все устройства іррр+	
	isdn+	Все устройства isdn+	
	ppp+	Все устройства ppp+	
	tun+	Все устройства tun+	
	wlan+	Все устройства wlan+	
< III >	Если вы вкли активирован	очите возможность маскарада, то для сетей IPv4 б ю перенаправление IP.	удет

Межсетевой экран включен. (изменен)

Рисунок 184 - Вкладка "Маскарад"

Изм.	Лист	№ докум	Подп	Дата

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 ІСМР:

- 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;

Изм.	Лист	№ докум	Подп	Дата

- 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.

🚽 Настройка межсетевого экрана _ 🗆 >								
<u>Ф</u> айл <u>П</u> араметры <u>С</u> правка								
Включить         Включить								
Доверенные службы Другие порты Доверенные интерф Маскарад         Протокол ICMP (Internet Control Message Protocol) обычно используется для обмена сообщениями об ошибках между компьютерами в сети, но с его помощью также можно отправлять информационные сообщения, такие как запросы и ответы ping.           Отметьте в списке типы ICMP, которым следует отказать в прохождении через межсетевой экран. По умолчанию ограничений нет.								
Перенаправление по фильтр ICMP         Тип ICMP         Тип протокола           Пользовательские п         Время превышено         ipv4, ipv6           Запрос маршрутизатора         ipv4, ipv6           Объявление маршрутизатора         ipv4, ipv6           Перенаправление         объявление маршрутизатора           Эзалрос маршрутизатора         ipv4, ipv6           Перенаправление         ipv4, ipv6           Эзалрос паравление         ipv4, ipv6           Объявление маршрутизатора         ipv4, ipv6           Проблема параметра         ipv4, ipv6           Эхо-запрос (пинг)         ipv4, ipv6           Эхо-ответ (ропд)         ipv4, ipv6								
(< ш ) L Межсетевой экран включен. (изменен)								

Рисунок 186 - Вкладка "Фильтр ІСМР"

Изм.	Лист	№ докум	Подп	Дата

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.

Файл Параметры Сп	Настройка межсетевого экрана равка	×
Мастер Примени	мть Перезагрузить Включить Выключить	
Доверенные службы Другие порты Доверенные интерф	Для добавления дополнительных правил межсетевого экран произвольные файлы с правилами. Эти файлы должны быть iptables-save.	а используйте в формате
Маскарад	Тип Таблица Имя файла	Добавить
Перенаправление по	🙀 Пользовательский файл прави 🗙	Изменить
Пользовательские п	Выберите тип протокола, таблицу межсетевого экрана и файл с	<u>У</u> далить
	Тип протокола: ipv4 🗘	Вверх
	Таблица экрана: mangle 😂	В <u>н</u> из
	Файл: (Нет)	
	Отменить	
< III >	Проверьте настройки межсетевого экрана после примене пользовательских правил.	ния
Межсетевой экран вкл	ючен. (изменен)	

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

Изм.	Лист	№ докум	Подп	Дата

#### ЦАУВ.14001-01 91 01

[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.

Σ	root@lo	ocalho	ost:/me	lia/MSV	Sph	ere_6.3_9	Server/F	ackages	;	_	×
<u>Ф</u> айл	<u>П</u> равка	<u>В</u> ид	П <u>о</u> иск	<u>Т</u> ермин	ал	<u>С</u> правка					
[root@l	ocalhost	Pack	ages]#								^
[root@l	ocalhost	Pack	ages]#	md5sum	aid	e-0.14-3.	sp6.2.x	86_64.rp	m		
873f633	dc5ea859	7d87d	l6cb43ac	:5e66f	aid	e-0.14-3.	sp6.2.x	86_64.rp	m		
[root@l	ocalhost	Pack	ages]#								
[root@l	ocalhost	Pack	ages]#								
[root@l	ocalhost	: Pack	ages]#	md5sum	che	ckpolicy-	2.0.22-	1.sp6.x8	6_64.r	pm	
099a1f8	371158a9c	f7adc	b82f6bf	fdfeca	che	ckpolicy-	2.0.22-	1.sp6.x8	6_64.r	pm	
[root@l	ocalhost	: Pack	ages]#								
[root@l	ocalhost	Pack	ages]#			1210121012121012	1. 1.1.1.1.1.1	0.00000			
[root@l	ocalhost	Pack	ages]#	md5sum	acl	-2.2.49-6	.sp6.x8	6_64.rpm			
tc3t525	669779b4	17d89e	0cf5930	:71†5b	acl	-2.2.49-6	.sp6.x8	6_64.rpm			_
[root@l	ocalhost	Pack	ages]#								=
[root@l	ocalhost	Pack	ages]#								$\sim$

Рисунок 188 – Проверка целостности пакетов

Изм.	Лист	№ докум	Подп	Дата

#### 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

Изм.	Лист	№ докум	Подп	Дата

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:

- #р: разрешения на файл
- #i: дескриптор inode
- #n: количество ссылок
- #и: 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)

Изм.	Лист	№ докум	Подп	Дата

#### ЦАУВ.14001-01 91 01

#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/\*

Изм.	Лист	№ докум	Подп	Дата

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

Изм.	Лист	№ докум	Подп	Дата

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.

🔘 Приложения Переход Система 🕹 🕸 🗾	😂 🕁	Срд, 16 Окт, 22:39	root
root@localhost:-/Рабочий стол Файл Правка Вид Поиск Терминал Справка Гооt@localhost Рабочий стол]#	d		
aide — Dolphin         gaán Правка Вид Перейти Серик: Настройка Справка         Kop         Hasag Вид Перейти Серик: Настройка Справка         Masag Big Cert         Corb         Masking Cold (Mustic)	CBECHEHUS & CBECHU		

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.

🔘 Приложения Переход Сист	ема 🔮 🥸 🗾	🔵 🗃 🏟	Чтв, 17 Окт, 02:41	root
E	root@localhost:~/Рабочий стол			• ×
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ер	минал <u>С</u> правка			
[root@localhost Рабочий стол]# ile database must have one db NIDE found differences between Start timestamp: 2013-10-17 02	aidecheck spec specification database and filesystem!! :40:35			^
Summary: Total number of files: Added files: Removed files: Changed files:	35 30 0 0			
\dded files:				
<pre>idded: /boot idded: /boot/initramfs-2.6.32-; idded: /boot/efi/EFI idded: /boot/efi/EFI/redhat idded: /boot/efi/FFI/redhat idded: /boot/fi/FFI/redhat/gri idded: /boot/fi/FFI/redhat/gri idded: /boot/grub/redhateri idded: /boot/grub/efs_stagel_1 idded: /boot/grub/device.map idded: /boot/grub/grub.conf idded: /boot/grub/grub.conf idded: /boot/grub/grub.conf idded: /boot/grub/frs_stagel_5 idded: /boot/grub/frs_stagel_5 idded: /boot/grub/frs_stagel_5 idded: /boot/grub/frs_stagel_5 idded: /boot/grub/frs_stagel_5 idded: /boot/grub/frs_stagel_5 idded: /boot/grub/frs_stagel_5 idded: /boot/grub/fa_stagel_5 idded: /boot/grub/fa_stagel_5 idded: /boot/grub/fa_stagel_5 idded: /boot/grub/fa_stagel_5 idded: /boot/grub/fa_stagel_5 idded: /boot/grub/fa_stagel_5 idded: /boot/grub/fa_stagel_5 idded: /boot/grub/fa_stagel_5</pre>	<pre>!79.22.1.sp6.x86_64.img lb.efi '9.22.1.sp6.x86_64.hmac .22.1.sp6.x86_64.gz .22.1.sp6.x86_64 ; ; 5 5</pre>			
<pre>added: /boot/grub/splash.xpm.g; added: /boot/grub/vstafs_stage</pre>	; L_5			=
added: /boot/grub/stage2				~

Рисунок 192 - Выполнение aide --check

Изм.	Лист	№ докум	Подп	Дата

Информацию о контрольных суммах, времени модификации контролируемых файлов и каталогов, можно будет увидеть в aide.db.gz (рис. 193).

<pre>aide.db</pre>	$\bigcirc$	Приложения Переход Система 🕹 🍥 🗹	чтв, 17 Окт, 03:00	roo
aide.db       aide.db - Ark             impair/owcenus       impair/owcenus       impair/owcenus       impair/owcenus       impair/owcenus         impair/owcenus       imp	×			
<pre>pabergin_db # This file was generated by Aide, version 0.14 # Time of generation was 2013-10-16 21:26:55 @edub_spec name lname attr perm uid gid size mtime ctime inode lcount md5 rmd160 sha256 acl xattrs selinux tiger /opt 0 12887002045 40755 0 0 4096 MTM4MTk2000yNQ== MTM4MTKY00WQ== 131074 30 0 0 POSIX, dXNLcjo6c14Cmdyb3Vw0jpyLXgKb3R /root 0 12887002045 40555 0 0 4096 MTM4MTK2000yNQ== MTM4MTKVVQ0== 131074 30 0 0 POSIX, dXNLcjo6c14Cmdyb3Vw0jpyLXgKb3R /rto 1 2887002045 40555 0 0 4096 MTM4MTK200TyNQ== MTM4MTKVVQ0== 131074 30 0 0 POSIX, dXNLcjo6c14Cmdyb3Vw0jpyLXgKb3R /rto 0 12887002045 40555 0 0 4096 MTM4MTK200TyNQ== MTM4MTKVVQ0== 131077 13 0 0 0 POSIX, dXNLcjo6c14Cmdyb3Vw0jpyLXgKb3R /rto 0 12887002045 40555 0 0 1022 BM MTM4MTK20TyNQ== MTM4MTKVVQ0== 653365 2 0 0 0 POSIX, dXNLcjo6c14Cmdyb3Vw0jpyLXgKb3RoZXI60 /lbi 0 12887002045 40555 0 0 1022 BM MTM4MTK20TyNA== MTM4MTKVVVNA== 5 0 0 0 POSIX, dXNLcjo6c14Cmdyb3Vw0jpyLXgKb3RoZXI6 /lbi 0 12887002045 40555 0 0 1222BM MTM4MTK20TYNA== MTM4MTKVVVNA== 0 0 0 0 POSIX, dXNLcjo6c14Cmdyb3Vw0jpyLXgKb3RoZXI6 /lsi 0 12887002045 40555 0 0 1224 BM MTM4TK20TYNA== MTM4MTKVVIXA== 76434 13 0 0 0 POSIX, dXNLcjo6c14Cmdyb3Vw0jpyLXgKb3RoZXI6 /lsi 0 12887002045 40555 0 0 10 0 0 0 31944 0 0 0 0 POSIX, dXNLcjo6cntCfmdyb3Vw0jpLXgKb3RoZXI60 /lst 0 4297064989 40755 0 0 0 0 0 0 31944 0 0 0 0 POSIX, dXNLcjo6cntCfmdyb3Vw0jpLXgKb3RoZXI60i1tLQ0=, 0 c c31zd6VtX3U6 /etc/rispig.conf 0 4297064989 100644 0 0 0 0 0 932947 0 0 0 0 POSIX, dXNLcjo6cntCfmdyb3Vw0jpLSKb3RoZXI60i1tLQ0=, 0 c c31zd6VtX /etc/hadow- 0 1396764349 100600 0 0 1 0 0 0 93247 0 0 0 0 POSIX, dXNLcjo6cntCfmdyb3Vw0jpLSKb3RoZXI60i1tLQ0=, 0 c c31zd6VtX /etc/hadow- 0 1396764349 100600 0 0 1 0 0 0 912512 0 0 0 0 POSIX, dXNLcjo6cntCfmdyb3Vw0jpLSKb3RoZXI60i1tLQ0=, 0 c c31zd6VtX /etc/hadow- 0 1396764349 100600 0 0 1 0 0 0 912512 0 0 0 0 POSIX, dXNLcjo6cntCfmdyb3Vw0jpLXgKb3RoZXI60i1tLQ0=, 0 c c31zd6VtX3U6 /etc/pang 0 4297064989 40755 0 0 0 0 0 912431 0 0 0 0 POSIX, dXNLcjo6cntCfmdyb3Vw0jpLXgKb3RoZXI60i1tLQ0=, 0 c c31zd6VtX3U6 /etc/pang 0 4297064989 4</pre>		аide.db текстовый документ		
		<pre>gBeegin_db</pre>	<pre>selinux tiger cnd4Cmdyb3Wu0jpyLXgkb doci14Cmdyb3Wu0jpyLXgkb doci14Cmdyb3Wu0jpyLXgkb cj06c114Cmdyb3Wu0jpyLXgkb cj06c114Cmdyb3Wu0jpyLXgkb3Roz Md4Cmdyb3Wu0jpyLXgkb3Roz Md4Cmdyb3Wu0jpyLXgkb3Roz Md4Cmdyb3Wu0jpyLXgkb3Roz Md4Cmdyb3Wu0jpyLXgkb3Roz iteAmdyb3Wu0jpyLXgkb3Roz Md4Cmdyb3Wu0jpyLXgkb3Roz iteAmdyb3Wu0jpyLXgkb3Roz Md4Cmdyb3Wu0jpLQkgkb3Roz Md4Cmdyb3Wu0jpLQkgkb3Roz Md4Cmdyb3Wu0jpLQkgkb3Roz Md4Cmdyb3Wu0jpLQkgkb3Roz Md4Cmdyb3Wu0jpLQkgkb3Roz Md4Cmdyb3Wu0jpLQkgkb3Roz Md4Cmdyb3Wu0jpLQkgkb3Roz Md4Cmdyb3Wu0jpLQkgkb3Roz Md4Cmdyb3Wu0jpLQkgkb3Roz Md4Cmdyb3Wu0jpLQkgkb3Roz Md4Cmdyb3Wu0jpLQkgkb3Roz Md4Cmdyb3Wu0jpLQkgkb3Roz Md4Cmdyb3Wu0jpLQkgkb3Roz Md4Cmdyb3Wu0jpLQkgkb3Roz Md4Cmdyb3Wu0jpLXgkb3Roz Md4Cmd4Cmdyb3Wu0jpLXgkb3Roz Md4Cmd4</pre>	Ro b3R grant
	- (			<u> </u>

Рисунок 193 - Результат проверки в файле aide.db.gz

Изм.	Лист	№ докум	Подп	Дата

### приложение

# ПЕРЕЧЕНЬ ПРОГРАММНЫХ ПАКЕТОВ, НЕОБХОДИМЫХ ДЛЯ ФУНКЦИОНИРОВАНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

1apr-util-Idap2bind-dyndb-Idap3checkpolicy4compat-openIdap5initscripts6ipa-server-selinux7iptables8iptables-devel9iptables-ipv610kernel11kernel-devel12kernel-firmware13kernel-headers14krb5-server-Idap15Idapjdk16libselinux-devel18libselinux-ruby20libselinux-ruby21libsemanage22mod_authz_Idap23module-init-tools24nss-pam-Idapd25openIdap-clients27openIdap-clevel28openIdap-servers	Nº	Наименование программного пакета
2bind-dyndb-ldap3checkpolicy4compat-openIdap5initscripts6ipa-server-selinux7iptables8iptables-devel9iptables-devel10kernel11kernel-devel12kernel-firmware13kernel-headers14krb5-server-ldap15ldapjdk16libselinux17libselinux-devel18libselinux-ruby20libselinux-ruby21libsemanage22mod_authz_ldap23module-init-tools24nss-pam-ldapd25openIdap-clients27openIdap-devel28openIdap-servers	1	apr-util-ldap
3checkpolicy4compat-openIdap5initscripts6ipa-server-selinux7iptables8iptables-devel9iptables-ipv610kernel11kernel-devel12kernel-firmware13kernel-headers14krb5-server-Idap15Idapjdk16libselinux17libselinux-devel18libselinux-ruby20libselinux-ruby21libsemanage22mod_authz_Idap23module-init-tools24nss-pam-Idapd25openIdap-clients27openIdap-devel28openIdap-servers	2	bind-dyndb-ldap
4compat-openIdap5initscripts6ipa-server-selinux7iptables8iptables-devel9iptables-ipv610kernel11kernel-devel12kernel-firmware13kernel-headers14krb5-server-ldap15ldapjdk16libselinux17libselinux-devel18libselinux-ruby20libselinux-ruby21libsemanage22mod_authz_ldap23module-init-tools24nss-pam-ldapd25openIdap-clients27openIdap-devel28openIdap-servers	3	checkpolicy
5initscripts6ipa-server-selinux7iptables8iptables-devel9iptables-ipv610kernel11kernel-devel12kernel-firmware13kernel-headers14krb5-server-ldap15ldapjdk16libselinux17libselinux-devel18libselinux-ruby20libselinux-ruby21libselinux-utils21libsemanage22mod_authz_ldap23module-init-tools24nss-pam-ldapd25openldap-clients27openldap-devel28openldap-servers	4	compat-openIdap
6ipa-server-selinux7iptables8iptables-devel9iptables-ipv610kernel11kernel-devel12kernel-firmware13kernel-headers14krb5-server-ldap15ldapjdk16libselinux17libselinux-devel18libselinux-ruby20libselinux-ruby21libsemanage22mod_authz_ldap23module-init-tools24nss-pam-Idapd25openIdap-clients27openIdap-devel28openIdap-servers	5	initscripts
7iptables8iptables-devel9iptables-ipv610kernel11kernel-devel12kernel-firmware13kernel-headers14krb5-server-ldap15ldapjdk16libselinux17libselinux-devel18libselinux-ruby20libselinux-ruby21libsemanage22module-init-tools24nss-pam-Idapd25openIdap-clients27openIdap-devel28openIdap-servers	6	ipa-server-selinux
8iptables-devel9iptables-ipv610kernel11kernel-devel12kernel-firmware13kernel-headers14krb5-server-ldap15Idapjdk16libselinux17libselinux-devel18libselinux-ruby20libselinux-ruby21libsemanage22mod_authz_Idap23module-init-tools24nss-pam-Idapd25openIdap-clients27openIdap-devel28openIdap-servers	7	iptables
9iptables-ipv610kernel11kernel-devel12kernel-firmware13kernel-headers14krb5-server-ldap15ldapjdk16libselinux17libselinux-devel18libselinux-ruby20libselinux-ruby21libsemanage22mod_authz_ldap23module-init-tools24nss-pam-ldapd25openldap-clients27openldap-devel28openldap-servers	8	iptables-devel
10kernel11kernel-devel12kernel-firmware13kernel-headers14krb5-server-ldap15ldapjdk16libselinux17libselinux-devel18libselinux-ruby20libselinux-ruby20libselinux-utils21libsemanage22mod_authz_ldap23module-init-tools24nss-pam-ldapd25openldap26openldap-clients27openldap-servers	9	iptables-ipv6
11kernel-devel12kernel-firmware13kernel-headers14krb5-server-ldap15ldapjdk16libselinux17libselinux-devel18libselinux-ruby20libselinux-ruby20libselinux-utils21libsemanage22mod_authz_ldap23module-init-tools24nss-pam-ldapd25openldap-clients27openldap-devel28openldap-servers	10	kernel
12kernel-firmware13kernel-headers14krb5-server-ldap15ldapjdk16libselinux17libselinux-devel18libselinux-ruby20libselinux-ruby20libselinux-utils21libsemanage22mod_authz_ldap23module-init-tools24nss-pam-ldapd25openldap26openldap-clients27openldap-servers	11	kernel-devel
13kernel-headers14krb5-server-ldap15ldapjdk16libselinux17libselinux-devel18libselinux-python19libselinux-ruby20libselinux-ruby21libsemanage22mod_authz_ldap23module-init-tools24nss-pam-ldapd25openldap26openldap-clients27openldap-devel28openldap-servers	12	kernel-firmware
14krb5-server-ldap15ldapjdk16libselinux17libselinux-devel18libselinux-python19libselinux-ruby20libselinux-ruby20libselinux-utils21libsemanage22mod_authz_ldap23module-init-tools24nss-pam-ldapd25openldap26openldap-clients27openldap-servers	13	kernel-headers
15ldapjdk16libselinux17libselinux-devel18libselinux-python19libselinux-ruby20libselinux-utils21libsemanage22mod_authz_ldap23module-init-tools24nss-pam-ldapd25openldap26openldap-clients27openldap-devel28openldap-servers	14	krb5-server-ldap
16libselinux17libselinux-devel18libselinux-python19libselinux-ruby20libselinux-utils21libsemanage22mod_authz_ldap23module-init-tools24nss-pam-ldapd25openldap26openldap-clients27openldap-devel28openldap-servers	15	ldapjdk
17libselinux-devel18libselinux-python19libselinux-ruby20libselinux-utils21libsemanage22mod_authz_ldap23module-init-tools24nss-pam-ldapd25openldap26openldap-clients27openldap-devel28openldap-servers	16	libselinux
18libselinux-python19libselinux-ruby20libselinux-utils21libsemanage22mod_authz_ldap23module-init-tools24nss-pam-ldapd25openldap26openldap-clients27openldap-devel28openldap-servers	17	libselinux-devel
19libselinux-ruby20libselinux-utils21libsemanage22mod_authz_ldap23module-init-tools24nss-pam-ldapd25openldap26openldap-clients27openldap-devel28openldap-servers	18	libselinux-python
20libselinux-utils21libsemanage22mod_authz_ldap23module-init-tools24nss-pam-ldapd25openldap26openldap-clients27openldap-devel28openldap-servers	19	libselinux-ruby
21libsemanage22mod_authz_ldap23module-init-tools24nss-pam-ldapd25openldap26openldap-clients27openldap-devel28openldap-servers	20	libselinux-utils
22mod_authz_ldap23module-init-tools24nss-pam-ldapd25openldap26openldap-clients27openldap-devel28openldap-servers	21	libsemanage
23module-init-tools24nss-pam-ldapd25openldap26openldap-clients27openldap-devel28openldap-servers	22	mod_authz_ldap
24nss-pam-ldapd25openldap26openldap-clients27openldap-devel28openldap-servers	23	module-init-tools
25openIdap26openIdap-clients27openIdap-devel28openIdap-servers	24	nss-pam-ldapd
26openIdap-clients27openIdap-devel28openIdap-servers	25	openIdap
27openIdap-devel28openIdap-servers	26	openIdap-clients
28 openIdap-servers	27	openldap-devel
	28	openIdap-servers

Изм.	Лист	№ докум	Подп	Дата

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

Изм.	Лист	№ докум	Подп	Дата

# 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)
СА	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)

Изм.	Лист	№ докум	Подп	Дата

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	Туре Enforcement (Соблюдение типов)
TTL	Time to live (Время жизни)
TOS	Туре of Service (Тип услуги)
UID	User Identifier (Идентификаторы пользователя)
URI	Uniform Resource Identifier (Унифицированный идентификатор ресурса)
URL	Uniform Resource Locator (Единообразный локатор ресурса)

Изм.	Лист	№ докум	Подп	Дата

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)
BM	Виртуальная машина
ИТ	Информационные технологии
OC	Операционная система
ПО	Программное обеспечение
ПЭВМ	Персональная электронно-вычислительная машина

Изм.	Лист	№ докум	Подп	Дата

# Лист регистрации изменений

	Номера листов (страниц)			Всего	Входящий Ма сопро				
Изм.	изменен- ных	заменен- ных	новых	аннулиро- ванных	листов (страниц) в докум.	листов № (страниц) докум в докум.	листов № водитель- По (страниц) докум. в докум. и дата	Подп.	іодп. Дата

Изм.	Лист	№ докум	Подп	Дата