

# Операционная система «РЕД ОС» Руководство администратора

RU.29926343.02.01-01 32 1-1

Copyright © 2020 ООО "РЕД СОФТ"

[HTTPS://REDOS.RED-SOFT.RU/](https://redos.red-soft.ru/)

Данный документ является руководством администратора операционной системы «РЕД ОС» версии 7.3 (далее РЕД ОС, ОС) и описывает действия по установке, настройке, запуску и использованию операционной системы, выполняемые администратором в процессе эксплуатации операционной системы. Также руководство администратора содержит описания:

- функций безопасного управления операционной системой;
- функций и интерфейсов, которые доступны администраторам операционной системы, связанным с администрированием;
- применения доступных администраторам функций безопасности, предоставляемых операционной системой.

Руководство администратора содержит предупреждения относительно доступных для администраторов функций и привилегий, которые следует контролировать в безопасной среде обработки информации.

*Первая публикация, декабрь 2020*

# Оглавление

## Общие сведения о РЕД ОС

<b>1</b>	<b>Общие сведения о РЕД ОС</b> .....	<b>8</b>
1.1	Описание и область применения операционной системы .....	8
1.2	Основные функции РЕД ОС .....	8
1.3	Состав РЕД ОС .....	10
1.4	Документация в составе .....	11
1.5	Требования к персоналу (администратору).....	11
1.5.1	Общие положения .....	11
1.5.2	Обязанности пользователей .....	12
1.6	Приёмка поставленного средства .....	13
<b>2</b>	<b>Разновидности файловых систем</b> .....	<b>15</b>
2.1	Поддерживаемые файловые системы.....	15
2.1.1	Утилиты для работы с файловыми системами .....	15
<b>3</b>	<b>Общие принципы работы РЕД ОС</b> .....	<b>18</b>
3.1	Процессы и файлы .....	18
3.1.1	Процессы функционирования РЕД ОС .....	19
3.1.2	Файловая система РЕД ОС .....	19
3.1.3	Организация файловой структуры .....	19
3.1.4	Иерархическая организация файловой системы .....	20

3.1.5	Имена дисков и разделов .....	21
<b>3.2</b>	<b>Работа с наиболее часто используемыми компонентами .....</b>	<b>22</b>
3.2.1	Командные оболочки (интерпретаторы) .....	22
<b>3.3</b>	<b>Использование многозадачности.....</b>	<b>25</b>
<b>3.4</b>	<b>Режимы работы ОС .....</b>	<b>26</b>
3.4.1	Диагностические режимы работы .....	26
3.4.2	Режимы отображения информации .....	28

## Установка РЕД ОС

<b>4</b>	<b>Установка РЕД ОС .....</b>	<b>31</b>
4.1	Начало установки .....	31
4.2	Альтернативные способы установки .....	33
4.2.1	Источники установки .....	34
4.2.2	Запуск сетевой установки .....	34
4.3	Последовательность установки .....	37
4.4	Язык .....	38
4.5	Обзор установки.....	38
4.6	Задание пароля администратора системы .....	45
4.7	Установка системы .....	47
4.8	Соглашение пользователя и Лицензионный договор .....	48
4.9	Завершение установки.....	49
4.10	Подготовительные процедуры .....	49

## Управление программным обеспечением

<b>5</b>	<b>Управление ПО .....</b>	<b>52</b>
5.1	Введение: пакеты, зависимости и репозитории .....	52
5.2	Основы работы с RPM .....	53
5.3	Назначение DNF .....	55
5.4	Источники программ (репозитории).....	56
5.5	Поиск пакетов .....	57
5.6	Установка или обновление пакета .....	57
5.7	Удаление установленного пакета .....	58
5.8	Обновление всех установленных пакетов .....	58
5.9	Puppet.....	58

<b>6</b>	<b>Система безопасности РЕД ОС</b>	<b>63</b>
<b>6.1</b>	<b>Программа sudo</b>	<b>63</b>
<b>6.2</b>	<b>IP-фильтр iptables: архитектура и синтаксис</b>	<b>63</b>
6.2.1	Устройство фильтра iptables	64
6.2.2	Встроенные таблицы фильтра iptables	64
6.2.3	Команды утилиты iptables	65
6.2.4	Ключи утилиты iptables	68
6.2.5	Основные действия над пакетами в фильтре iptables	68
6.2.6	Основные критерии пакетов в фильтре iptables	70
6.2.7	Использование фильтра iptables	72
<b>6.3</b>	<b>Аудит в РЕД ОС</b>	<b>72</b>
6.3.1	Файлы и утилиты аудита РЕД ОС	72
<b>6.4</b>	<b>Права доступа к файлам и каталогам</b>	<b>94</b>
6.4.1	chmod	97
6.4.2	umask	100
6.4.3	chown	100
6.4.4	ACL	101
6.4.5	Chattr и lsattr	103
<b>6.5</b>	<b>Systemd – управление компонентами ОС</b>	<b>105</b>
<b>6.6</b>	<b>SELinux</b>	<b>109</b>
6.6.1	Введение	109
6.6.2	Установка	110
6.6.3	Утилиты	110
<b>6.7</b>	<b>РАМ</b>	<b>130</b>
<b>6.8</b>	<b>Rsyslog</b>	<b>138</b>
<b>6.9</b>	<b>Afick - верификация целостности</b>	<b>142</b>
<b>6.10</b>	<b>AMTU - утилита тестирования абстрактной машины</b>	<b>146</b>
<b>6.11</b>	<b>ntpdate</b>	<b>147</b>
<b>6.12</b>	<b>Отказоустойчивый кластер</b>	<b>150</b>
<b>6.13</b>	<b>Изменение приоритета процесса</b>	<b>154</b>
<b>6.14</b>	<b>Управление дисковыми квотами</b>	<b>156</b>
<b>6.15</b>	<b>Ограничение ресурсов пользователя</b>	<b>161</b>
<b>6.16</b>	<b>Контроль целостности запускаемых компонентов</b>	<b>162</b>
<b>6.17</b>	<b>Блокирование файлов</b>	<b>164</b>
<b>6.18</b>	<b>Очистка памяти</b>	<b>164</b>
6.18.1	shred	164
6.18.2	wipe	165
6.18.3	Secure-Delete	167

6.19	Экспорт данных пользователя.....	169
6.20	Резервирование данных .....	171
6.21	Лимиты ресурсов.....	171
6.22	Монтирование файловых систем .....	172
6.23	Принудительное завершение сеанса пользователя.....	174

## Управление пользователями

<b>7</b>	<b>Управление пользователями .....</b>	<b>176</b>
7.1	Общая информация .....	176
7.2	Утилита passwd.....	177
7.3	Добавления нового пользователя .....	177
7.4	Модификация пользовательских записей.....	181
7.5	Удаление пользователей.....	181
7.6	Пароли пользователей.....	182
7.7	Роли пользователей .....	186

## Сеть и служебные программы

<b>8</b>	<b>Настройка сети .....</b>	<b>195</b>
<b>9</b>	<b>Служебные программы .....</b>	<b>200</b>
9.1	Служба xinetd.....	200
9.1.1	Параметры .....	201
9.1.2	Управление xinetd .....	202
9.1.3	Файлы .....	203
9.2	Crontab.....	203
9.3	Полноэкранный редактор vi.....	206
9.3.1	Режимы работы редактора .....	206
9.3.2	Ввод текста .....	206
9.3.3	Команды .....	206
9.3.4	Перемещение курсора .....	207
9.3.5	Редактирование .....	207
9.3.6	Командная строка .....	207
9.3.7	Блоки, буферы, окна редактирования. Повторители .....	208
9.3.8	Открыть/создать файл .....	209
9.3.9	Дополнительные опции .....	210
9.4	Редактор VIM.....	210
9.4.1	Режимы работы .....	210
9.4.2	Основные возможности .....	211
9.4.3	Конфигурация .....	213

# Общие сведения о РЕД ОС

# 1. Общие сведения о РЕД ОС

## 1.1 Описание и область применения операционной системы

РЕД ОС является многопользовательской, многозадачной ОС, которая предоставляет платформу унифицированной функциональной универсальной доверенной среды для выполнения прикладного программного обеспечения.

РЕД ОС на уровне драйверов поддерживает широкий перечень оборудования актуальных версий, доступного на рынке СВТ, а так же оборудования снятого с производства, но поддерживаемого производителями.

В РЕД ОС поддерживается инсталляция с оптических носителей информации, флеш-накопителей, разделов локального жёсткого диска, а так же установка по сети передачи данных.

## 1.2 Основные функции РЕД ОС

РЕД ОС может обеспечивать обслуживание от одного до нескольких пользователей одновременно. После успешного входа в систему пользователи имеют доступ в главную вычислительную среду, позволяющую запускать пользовательские приложения, создавать и получать доступ к файлам, задавать директивы пользователя на уровне оболочки командного процессора. РЕД ОС предоставляет адекватные механизмы для разграничения пользователей и защиты их данных. Использование привилегированных команд ограничено и доступно только административным пользователям.

РЕД ОС конфигурируется по умолчанию для работы в режиме дискреционного управления доступом (DAC).

Любой пользователь с ролью, которая позволяет выполнять административные действия, считается административным пользователем. Кроме того, РЕД ОС поддерживает типы, которые могут быть связаны с объектами, и домены,

которые могут быть связаны с процессами. Роли определяются доменами, к которым они имеют доступ. Предопределённый файл политики, который является частью конфигурации РЕД ОС, определяет правила между доменами и типами. С вышеизложенным определением ролей и прав доступа, подразумеваемых индивидуальными ролями, РЕД ОС выполняет требования ролевого доступа.

РЕД ОС предназначена для работы в сетевом окружении с другими экземплярами РЕД ОС, а также с иными совместимыми серверными и клиентскими системами одного и того же управляемого домена. Все эти системы должны конфигурироваться в соответствии с определённой общей политикой безопасности.

РЕД ОС разрешает использование многими пользователями одного или более процессоров, присоединённых внешних и запоминающих устройств для выполнения разнообразных функций, требующих управляемого распределённого доступа к данным, хранимым в системе. Такие инсталляции типичны для вычислительных систем рабочих групп или предприятий, к которым обращаются локальные пользователи, или компьютерных систем с иначе защищённым доступом.

Предполагается, что ответственность за сохранение данных, защищаемых РЕД ОС, может делегироваться пользователям РЕД ОС. Все данные находятся под управлением механизмов безопасности РЕД ОС. Данные сохраняются в поименованных объектах, и РЕД ОС может связать с каждым поименованным объектом описание прав доступа к этому объекту. Всем пользователям назначаются уникальные идентификаторы. Этот идентификатор пользователя используется вместе с атрибутами и ролями, назначенными пользователю, как основание для решений по управлению доступом. РЕД ОС подтверждает подлинность предъявленного идентификатора пользователя до того, как разрешать ему выполнять дальнейшие действия. РЕД ОС внутри себя сопровождает ряд идентификаторов, связанных с процессами, которые получаются из уникального идентификатора пользователя, предъявляемого при входе в систему. Некоторые из этих идентификаторов могут изменяться во время выполнения процесса согласно политике, реализуемой РЕД ОС.

РЕД ОС предоставляет такие меры безопасности, при которых доступ к объектам данных осуществляется только в соответствии с ограничениями на доступ, наложенными на этот объект его владельцем, административными пользователями и типом объекта. Права владения на поименованные объекты могут передаваться под контролем политики управления доступом.

На объекты данных могут быть назначены дискреционные права доступа (например, чтение, запись, выполнение) субъектов (пользователей). Как только субъекту предоставляется доступ к объекту, его содержание может быть свободно использовано для воздействия на другие доступные этому субъекту объекты.

РЕД ОС имеет существенные расширения элементов безопасности по сравнению со стандартными системами UNIX:

- списки управления доступом;
- реализацию доменов и типов;
- журналируемая файловая система (ext4);
- подключаемые модули аутентификации (PAM);
- специализированная система аудита, которая позволяет учитывать критические события безопасности и предоставляет административному пользо-

вателю инструментальные средства конфигурирования системы аудита и оценки записей аудита;

- базовые функции проверки комплекта оборудования позволяют по требованию административного пользователя проверять, правильно ли обеспечиваются основные функции безопасности аппаратных средств, на которые полагается ОО.

Развёрнутую ОС применяют в качестве программной платформы для разработок защищённых систем, требования к безопасности которых не превышают указанных показателей. В частности, такие требования предъявляются к защищённым программным системам, работающим с конфиденциальной информацией и персональными данными.

### 1.3 Состав РЕД ОС

РЕД ОС состоит из набора компонентов, предназначенных для реализации функциональных задач, необходимых пользователям (должностным лицам) для выполнения определенных должностными инструкциями повседневных действий, и поставляется в виде дистрибутива и комплекта эксплуатационной документации.

В структуре РЕД ОС можно выделить следующие функциональные элементы:

- ядро ОС;
- системные библиотеки;
- встроенные средства защиты информации (КСЗ);
- системные приложения;
- программные серверы;
- прочие серверные программы;
- интерактивные рабочие среды и командные интерпретаторы;
- прочие системные приложения.

Комплекс встроенных средств защиты информации, является принадлежностью операционной среды РЕД ОС и неотъемлемой частью ядра ОС и системных библиотек.

Ядро ОС – программа (набор программ), выполняющая функции управления ОС и взаимодействия ОС с аппаратными средствами.

Системные библиотеки – наборы программ (пакетов программ), выполняющие различные функциональные задачи и предназначенные для их динамического подключения к работающим программам, которым необходимо выполнение этих задач.

Встроенные средства защиты информации – специальные пакеты программ ОС, входящие в состав ядра ОС и системных библиотек, предназначенные для защиты ОС от несанкционированного доступа к обрабатываемой (хранящейся) информации на ЭВМ.

Системные приложения – это приложения (программы, набор программ), предназначенные для выполнения (оказания) системных услуг пользователю при решении им определенных функциональных задач в работе с операционной средой и обеспечивающие их выполнение.

Программные серверы – специальные приложения, предназначенные для предоставления пользователю определенных услуг и обеспечивающие их выполнение.

К прочим серверным программам относятся программы, предоставляющие пользователю различные услуги по обработке, передаче, хранению информации (серверы протоколов, почтовые серверы, серверы приложений, серверы печати и прочие).

Интерактивные рабочие среды (ИРС) – программы (пакеты программ), предназначенные для работы пользователя в РЕД ОС и предоставляющие ему удобный интерфейс для общения с ней. Командные рабочие среды включают в свой состав командные интерпретаторы.

Командные интерпретаторы – специальные программы (терминалы), предназначенные для выполнения различных команд, подаваемых пользователем при работе с РЕД ОС.

Прочие системные приложения – приложения (программы), оказывающие пользователю дополнительные системные услуги при работе с ОС.

В состав РЕД ОС включены следующие дополнительные системные приложения:

- архиваторы;
- приложения для управления RPM-пакетами;
- приложения мониторинга системы;
- приложения для работы с файлами;
- приложения для настройки системы;
- настройка параметров загрузки;
- настройка оборудования;
- настройка сети.

## 1.4 Документация в составе

В составе РЕД ОС представлена следующая документация:

- Электронная, контекстно-зависимая справочная система;
- Электронные справочники (man).

## 1.5 Требования к персоналу (администратору)

### 1.5.1 Общие положения

Администратор РЕД ОС должен иметь:

- базовые навыки администрирования ОС семейства Linux;
- навыки конфигурирования и настройки программных продуктов и ОС;
- опыт работы со стандартными элементами графического интерфейса приложений;
- навыки поддержания в работоспособном состоянии технических средств ПК.

### 1.5.2 Обязанности пользователей, определяемые предположениями безопасности

#### Предопределённое использование РЕД ОС

Доступ администраторов к РЕД ОС должен осуществляться только из санкционированных точек доступа – рабочих мест, размещённых в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

Для предотвращения несанкционированного доступа к системным компонентам пользователей РЕД ОС администраторы обязаны предотвращать и выявлять установку и запуск встроенных программ отладки.

Администраторы обязаны производить установку только штатных программных средств, не позволяющих осуществить несанкционированную модификацию ОО.

При взаимодействии с внешними информационными системами администраторы, при помощи средств РЕД ОС, должны осуществлять настройку взаимодействия только с доверенными системами, ПБ которых скоординированы с ПБ рассматриваемой РЕД ОС.

При возникновении сбоев и отказов СВТ или РЕД ОС администраторы обязаны предпринимать меры, направленные на восстановление безопасного состояния программного и аппаратного обеспечения РЕД ОС, в соответствии с данным Руководством.

Установка, конфигурирование и управление РЕД ОС должны осуществляться администратором РЕД ОС, в соответствии с настоящим документом. Самостоятельные действия по установке, конфигурированию и управлению пользователям не доступны и ограничены правилами разграничения доступа РЕД ОС.

#### Порядок обеспечения среды функционирования РЕД ОС

Администраторы должны использовать функции, предоставляемые РЕД ОС, в рамках выполнения своих должностных обязанностей, определенных в должностной инструкции соответствующих категорий пользователей.

Администраторы обязаны производить настройку оборудования СВТ и предотвращать несанкционированную физическую модификацию аппаратного обеспечения, на котором выполняется РЕД ОС.

Права пользователей для получения доступа и выполнения обработки информации в РЕД ОС основываются на одной или более ролях и назначаются администратором РЕД ОС. Роли пользователей в РЕД ОС отражают производственную функцию, обязанности, квалификацию и/или компетентность пользователей в рамках организации.

По всем вопросам администрирования РЕД ОС пользователь обязан обращаться к администраторам РЕД ОС, которые являются компетентными, хорошо обученными и заслуживающими доверия.

Предполагается наличие (одного или более) компетентных лиц (администраторов), которые назначаются для управления безопасностью РЕД ОС и информации в нем. Они несут ответственность за следующие функции:

- создание и сопровождение ролей;
- установление и сопровождение отношений между ролями;
- назначение и аннулирование ролей, назначаемых пользователям.

Кроме того, эти лица (в качестве владельцев всех корпоративных данных), наряду с владельцами объекта, должны иметь возможность назначать и отменять права доступа ролей к объектам.

Пользователи, в соответствии с назначенными в РЕД ОС полномочиями и ролями, имеют права создавать новые объекты данных, владельцами которых они становятся.

Персонал, ответственный за выполнение администрирования РЕД ОС, должен пройти проверку на благонадёжность и в своей деятельности должен руководствоваться документацией на РЕД ОС.

Уполномоченные пользователи обладают необходимым разрешением на доступ в РЕД ОС, по крайней мере, к части информации, управляемой РЕД ОС, и согласованно действуют в благоприятной среде.

Администраторы в обязательном порядке должны быть ознакомлены с настоящим руководством и должны быть обучены применению функциональных возможностей безопасности, предоставляемых операционной системой.

Администраторы должны выполнять группы задач, связанных со своими служебными полномочиями, в безопасной ИТ-среде с применением полного управления своими данными.

Администраторы должны осуществлять регулярный контроль полноты и достаточности мер по обеспечению информационной безопасности на объектах, использующих РЕД ОС.

## 1.6 Приёмка поставленного средства

Для контроля качества и приёмки РЕД ОС силами потребителя производятся испытания полученного изделия. При этом производится проверка контрольных сумм дистрибутива РЕД ОС. Снятие КС должно осуществляться с использованием ПО РСП-Контроль версии 2.0, по алгоритму ГОСТ 34.11-2012 (256 бит). Полученные КС должны соответствовать эталонным КС РЕД ОС, приведённым в формуляре.

Состав и последовательность испытаний:

1. Проверка общих требований.
2. Проверка комплектности.
3. Проверка маркировки и упаковки.
4. Проверка документации.
5. Проверка носителей данных.

Для проверки комплектности необходимо осуществить сверку состава предъявленного на испытания изделия с комплектностью:

- РЕД ОС. Дистрибутив,
- РЕД ОС. Дополнительный диск,
- РЕД ОС. Формуляр,
- Копия сертификата ФСТЭК России,

представленных на физических носителях или в виде электронных файлов.

Изделие считается соответствующим требованиям, если состав предъявленного на испытания изделия соответствует указанной комплектности.

В качестве носителей дистрибутивного комплекта РЕД ОС на физических носителях должны использоваться цифровые многоцелевые диски (DVD), не имеющие видимых механических повреждений, отрицательно влияющих на процессы воспроизведения информации. Носители РЕД ОС считаются прошедшими проверку, если установлено, что они соответствуют указанным требованиям.

В состав документации РЕД ОС должны входить документы:

- Операционная система «РЕД ОС» Формуляр. RU.29926343.02.01-01 30;
- Операционная система «РЕД ОС» Руководство администратора. RU.29926343.02.01-01 32 1-1;
- Операционная система «РЕД ОС» Руководство пользователя. RU.29926343.02.01-01 34 1-1.

Документация считается прошедшей проверку, если ее состав соответствует указанным требованиям.

Цифровые многоцелевые диски (DVD) с размещённой на них РЕД ОС должны быть промаркированы и упакованы. Маркировка цифровых многоцелевых дисков с размещённой на них РЕД ОС должна наноситься на внешнюю (нерабочую) поверхность диска и обязательно содержать наименование изделия и серийный номер, позволяющие однозначно идентифицировать РЕД ОС. Сертифицированные образцы должны быть маркированы специальным защитным знаком Системы сертификации СЗИ по требованиям безопасности информации № РОСС RU. 0001.01БИ00, наносимым в разделе 8 Формуляра RU.29926343.02.01-01 30. Для проверки маркировки и упаковки РЕД ОС необходимо удостовериться в их соответствии указанным требованиям.

Если в процессе испытаний будет обнаружено несоответствие хотя бы одному требованию, то принимаемый экземпляр РЕД ОС считается не выдержавшим испытания и возвращается для выявления причин дефектов.

РЕД ОС считается окончательно принятой, если она соответствует требованиям и успешно прошла испытания.

## 2. Разновидности файловых систем

### 2.1 Поддерживаемые файловые системы

В дистрибутиве поддерживаются следующие файловые системы (ФС):

- журналируемая файловая система ext3;
- журналируемая файловая система ext4;
- файловая система ISO 9660 для накопителей для оптических магнитных дисков.

#### 2.1.1 Утилиты для работы с файловыми системами

Общее назначение утилит приведено в таблице.

Утилита	Назначение
<code>mkfs</code>	создание новой файловой системы (make filesystem);
<code>fsck</code>	проверка файловой системы на ошибки (filesystem check);
<code>df</code>	формирует отчёт о доступном и использованном дисковом пространстве на файловых системах. Без аргументов <code>df</code> выдаёт отчёт по доступному и использованному пространству для всех файловых систем (всех типов), которые смонтированы в данный момент. В противном случае, <code>df</code> на каждый файл, заданный как аргумент, выдаётся отчёт по файловой системе, которая его содержит;

Утилита	Назначение
du	формирует отчёт об использовании дискового пространства заданными файлами, а также каждым каталогом иерархии подкаталогов каждого указанного каталога. Здесь под использованным дисковым пространством понимается пространство, используемое для всей иерархии подкаталогов указанного каталога. Запущенная без аргументов команда du выдаёт отчёт о дисковом пространстве для текущего каталога.

Для различения файловых систем используется указание типа файловой системы после параметра `-t` или в качестве компонента имени утилиты, например:

```
mkfs -t ext2 /dev/sda1
fsck.ext2 /dev/sda2
```

Для преобразования файловой системы из `ext2` в `ext3` необходимо выполнить команду:

```
tune2fs -j /dev/sd<X>
```

Для обратного преобразования необходимо смонтировать этот раздел как `ext2`.

Для того, чтобы сохранить копию диска (например, CD-ROM), необходимо сделать следующее:

- убедиться в наличии в текущем каталоге достаточного количества свободного места;
- выполнить команду:

```
dd if=/dev/cdrom of=cdrom.iso bs=1M
```

- после этого можно просмотреть содержимое файла `cdrom.iso`, смонтировав его, например, так:

```
mount -o loop cdrom.iso /mnt/cdrom
```

В качестве исходного устройства для копирования также может выступать любое дисковое устройство, например, дискета или жёсткий диск. Кроме того, получившийся образ CD-ROM можно записать на матрицу CD-R/RW с использованием команды `cdrecord`, т.к. файл `cdrom.iso` является полным образом диска.

Справочник наиболее часто используемых утилит для работы с файловой системой приведен в таблице.

Системный вызов	Назначение
mount	монтирование файловых систем;

Системный вызов	Назначение
umount	размонтирование файловых систем;
find	поиск файлов в директориях;
locate	поиск файлов по определённому образцу имени;
which	поиск файла, который будет запущен при выполнении данной команды;
cd	смена текущего каталога/директории;
pwd	показать текущий каталог/директорию;
mkdir	создание каталога;
ls	выдача информации о файлах или каталогах;
cp	копирование файлов;
mv	перемещение/переименование файлов;
rm	удаление файлов;
cat	вывод содержимого заданных файлов на стандартный вывод;
more	программа постраничного просмотра файлов;
ln	создание ссылок (альтернативных имён) для файлов;
file	определение типа файла;
chmod	изменение прав доступа к файлам;
chown	смена прав владения (пользовательских и групповых) для файлов;
umask	установка маски прав доступа для вновь создаваемых файлов;
chattr	изменение атрибутов файлов для файловой системы ext (append-only, immutable, safe deletion, no atime modified, no backup,...);
lsattr	просмотр атрибутов файлов для файловой системы ext.

## 3. Общие принципы работы РЕД ОС

Работа с операционной средой заключается во вводе определенных команд (запросов) к операционной среде и получению на них ответов в виде текстового отображения.

Диалог с ОС осуществляется посредством командных интерпретаторов с системных библиотек. Каждая системная библиотека представляет собой набор программ, динамически вызываемых операционной системой.

Для удобства пользователей при работе с командными интерпретаторами используются интерактивные рабочие среды (ИРС), предоставляющие пользователю удобный интерфейс для работы с ОС.

В самом центре ОС РЕД ОС находится управляющая программа, называемая ядром. Ядро взаимодействует с компьютером и периферией (дисками, принтерами и т.д.), распределяет ресурсы и выполняет фоновое планирование заданий. Другими словами, ядро ОС изолирует пользователя от сложностей аппаратуры компьютера, командный интерпретатор от ядра, а ИРС от командного интерпретатора.

### 3.1 Процессы и файлы

РЕД ОС является многопользовательской интегрированной системой. Это значит, что она разработана с расчётом на одновременную работу нескольких пользователей.

Пользователь может либо сам работать в системе, выполняя некоторую последовательность команд, либо от его имени могут выполняться прикладные процессы.

Пользователь взаимодействует с системой через командный интерпретатор, который представляет собой, как было сказано выше, прикладную программу, которая принимает от пользователя команды или набор команд и транслирует

их в системные вызовы к ядру системы. Интерпретатор позволяет пользователю просматривать файлы, передвигаться по дереву файловой системы, запускать прикладные процессы. Все командные интерпретаторы имеют развитый командный язык и позволяют писать достаточно сложные программы, упрощающие процесс администрирования системы и работы с ней.

### 3.1.1 Процессы функционирования РЕД ОС

Все программы, которые выполняются в текущий момент времени, называются процессами. Процессы можно разделить на два основных класса: системные процессы и пользовательские процессы.

Системные процессы - программы, решающие внутренние задачи РЕД ОС, например организацию виртуальной памяти на диске или предоставляющие пользователям те или иные сервисы (процессы-службы).

Пользовательские процессы - процессы, запускаемые пользователем из командного интерпретатора для решения задач пользователя или управления системными процессами.

Фоновый режим работы процесса - режим, когда программа может работать без взаимодействия с пользователем. В случае необходимости интерактивной работы с пользователем (в общем случае) процесс будет «остановлен» ядром и работа его продолжится только после перевода его в «нормальный» режим работы.

### 3.1.2 Файловая система РЕД ОС

В ОС использована файловая система, которая является единым деревом. Корень этого дерева - каталог, называемый root (рут), и обозначаемый «/». Части дерева файловой системы могут физически располагаться в разных разделах разных дисков или вообще на других компьютерах, - для пользователя это прозрачно. Процесс присоединения файловой системы раздела к дереву называется монтированием, удаление - размонтированием.

Например, файловая система CD-ROM в РЕД ОС монтируется по умолчанию в каталог /media/cdrom (путь в РЕД ОС обозначается с использованием «/», а не «\», как в DOS/Windows). Текущий каталог обозначается «./».

### 3.1.3 Организация файловой структуры

Система домашних каталогов пользователей помогает организовывать безопасную работу пользователей в многопользовательской системе. Вне своего домашнего каталога пользователь обладает минимальными правами (обычно чтение и выполнение файлов) и не может нанести ущерб системе, например, удалив или изменив файл.

Кроме файлов, созданных пользователем, в его домашнем каталоге обычно содержатся персональные конфигурационные файлы некоторых программ.

Маршрут (путь) - это последовательность имён каталогов, представляющий собой путь в файловой системе к данному файлу, где каждое следующее имя отделяется от предыдущего наклонной чертой (слэшем). Если название маршрута начинается со слэша, то путь в искомый файл начинается от корневого каталога всего дерева системы. В обратном случае, если название маршрута начинается

непосредственно с имени файла, то путь к искомому файлу должен начинаться от текущего каталога (рабочего каталога).

Имя файла может содержать любые символы за исключением кривой черты (/). Однако следует избегать применения в именах файлов большинства знаков препинания и непечатаемых символов. При выборе имен файлов рекомендуем ограничиться следующими символами:

- строчные и ПРОПИСНЫЕ буквы. Следует обратить внимание на то, что регистр всегда имеет значение;
- символ подчёркивания ( \_ );
- точка ( . ).

Для удобства работы можно использовать знак «.» (точка) для отделения имени файла от расширения файла. Данная возможность может быть необходима пользователям или некоторым программам, но не имеет значения для shell.

### 3.1.4 Иерархическая организация файловой системы

Содержимое корневого каталога «/» представлено в таблице.

Каталог	Описание каталога
/boot	место, где хранятся файлы, необходимые для загрузки ядра системы;
/lib	здесь располагаются файлы динамических библиотек, необходимых для работы большей части приложений, и подгружаемые модули ядра;
/bin	минимальный набор программ, необходимых для работы в системе;
/sbin	набор программ для административной работы с системой (программы, необходимые только суперпользователю);
/home	здесь располагаются домашние каталоги пользователей;
/etc	в данном каталоге обычно хранятся общесистемные конфигурационные файлы для большинства программ в системе;
/etc/rc?.d, /etc/init.d, /etc/rc.boot, /etc/rc.d	директории, где расположены командные файлы, выполняемые при запуске системы или при смене ее режима работы;
/etc/passwd	база данных пользователей, в которой содержится информация об имени пользователя, его настоящем имени, личном каталоге, зашифрованный пароль и другие данные;
/etc/shadow	тенивая база данных пользователей. При этом информация из файла /etc/passwd перемещается в /etc/shadow, который недоступен по чтению всем, кроме пользователя root;
/dev	в этом каталоге находятся файлы устройств. Файлы в /dev создаются сервисом udev;

Каталог	Описание каталога
<code>/usr</code>	обычно файловая система <code>/usr</code> достаточно большая по объёму, так как все программы установлены именно здесь. Вся информация в каталоге <code>/usr</code> помещается туда во время установки системы. Отдельно устанавливаемые пакеты программ и другие файлы размещаются в каталоге <code>/usr/local</code> . Некоторые подкаталоги системы <code>/usr</code> рассмотрены ниже;
<code>/usr/bin</code>	практически все команды, хотя некоторые находятся в <code>/bin</code> или в <code>/usr/local/bin</code> ;
<code>/usr/sbin</code>	команды, используемые при администрировании системы и не предназначенные для размещения в файловой системе <code>root</code> ;
<code>/usr/local</code>	здесь рекомендуется размещать файлы, установленные без использования пакетных менеджеров, внутренняя организация каталогов практически такая же, как и у корневого каталога;
<code>/usr/man</code>	каталог, где хранятся файлы справочного руководства <code>man</code> ;
<code>/usr/share</code>	каталог для размещения общедоступных файлов большей части приложений.

Содержимое каталога «`/var`» представлено в таблице.

Каталог	Описание каталога
<code>/var/log</code>	место, где хранятся файлы аудита работы системы и приложений;
<code>/var/spool</code>	каталог для хранения файлов, находящихся в очереди на обработку для того или иного процесса (очередь на печать, отправку почты и т.д.);
<code>/tmp</code>	временный каталог, необходимый некоторым приложениям;
<code>/proc</code>	файловая система <code>/proc</code> является виртуальной и в действительности не существует на диске. Ядро создаёт её в памяти компьютера. Система <code>/proc</code> предоставляет информацию о системе.

### 3.1.5 Имена дисков и разделов

Все физические устройства компьютера отображаются в каталоге `/dev` файловой системы РЕД ОС. Диски (в том числе IDE/SATA/SCSI жесткие диски, USB-диски) имеют имена:

- `/dev/sda` - первый диск;
- `/dev/sdb` - второй диск и т.д.

Диски обозначаются `/dev/sdX`, где X - a,b,c,d,e,... в зависимости от порядкового номера диска на шине.

Раздел диска обозначается числом после его имени.

Например, /dev/sdb4 - четвёртый раздел второго диска.

## 3.2 Работа с наиболее часто используемыми компонентами

### 3.2.1 Командные оболочки (интерпретаторы)

Как было сказано выше, для управления ОС используются командные интерпретаторы (shell).

Зайдя в систему, пользователь увидит приглашение - строку, содержащую символ «\$» (далее этот символ будет обозначать командную строку). Программа ожидает ввода команд. Роль командного интерпретатора - передавать команды операционной системе. При помощи командных интерпретаторов можно писать небольшие программы - сценарии (скрипты). В РЕД ОС используется командная оболочка Bash (Bourne Again Shell). Она ведёт историю команд и предоставляет возможность их редактирования.

Чтобы проверить, какую оболочку Вы используете, наберите команду:

```
echo $SHELL
```

У каждой командной оболочки свой синтаксис команд. В РЕД ОС рекомендуется использовать командную оболочку Bash. Дальнейшее описание и примеры будут приведены с использованием данной командной оболочки.

#### Командная оболочка Bash

В bash имеется несколько приёмов для работы со строкой команд. Например, используя клавиатуру, можно:

- Ctrl + A – перейти на начало строки.
- Ctrl + U – удалить текущую строку.
- Ctrl + C – остановить текущую задачу.

Можно использовать «;» для того, чтобы ввести несколько команд одной строкой. Клавиши «вверх» и «вниз», позволяют перемещаться по истории команд. Для того, чтобы найти конкретную команду в списке набранных, не пролистывая всю историю, нужно набрать:

Ctrl + R

Команды, присутствующие в истории, отображаются в списке пронумерованными. Для того, чтобы запустить конкретную команду, нужно набрать:

```
! <номер_команды>
```

если будет введено:

```
!!
```

запустится последняя из набранных команд.

Иногда имена программ и команд слишком длинны, но Bash сам может завершать имена. Нажав клавишу «ТАБ», можно завершить имя команды,

программы или каталога. Предположим, необходимо использовать программу декомпрессии `bunzip2`. Для этого нужно набрать:

```
bu
```

затем нажать «TAB». Если ничего не происходит, то, вероятно, существует несколько возможных вариантов завершения команды.

Нажав клавишу «TAB» ещё раз, можно получить список имён, начинающихся с «bu».

Например:

```
bu buildhash builtin bunzip2
```

Если далее добавить «n» (`bunzip2` - это единственное имя, третьей буквой которого является «n»), а затем нажать клавишу «TAB», оболочка дополнит имя и остаётся лишь нажать «Enter», чтобы запустить команду.

Заметим, что программу, вызываемую из командной строки, Bash ищет в каталогах, определяемых в системной переменной PATH. По умолчанию, в этот перечень каталогов не входит текущий каталог, обозначаемый «./» (точка слэш). Поэтому, для запуска программы `prog` из текущего каталога, надо дать команду:

```
./prog
```

### Базовые команды оболочки Bash

Все команды, приведённые ниже, могут быть запущены в режиме консоли.

Для получения более подробной информации используйте команду «man». Например:

```
man ls
```

Команда «su» позволяет получить права администратора. Когда пользователь набирает «su», оболочка запрашивает пароль суперпользователя (root). Необходимо ввести пароль и нажать «Enter». Чтобы вернуться к правам основного пользователя, необходимо набрать «exit».

Команда «cd» позволяет сменить каталог. Она работает как с абсолютными, так и с относительными путями. Предположим, что находясь в своём домашнем каталоге, пользователь хочет перейти в его подкаталог `docs/`. Для этого нужно ввести относительный путь:

```
cd docs/
```

Чтобы перейти в каталог `/usr/bin`, нужно набрать (абсолютный путь):

```
cd /usr/bin/
```

Некоторые варианты команды приведены в таблице.

Команда	Описание команды
<code>cd ..</code>	позволяет сделать текущим родительский каталог;
<code>cd -</code>	позволяет вернуться в предыдущий каталог;
<code>cd</code> <без_параметров>	переводит в домашний каталог.

Команда «ls» (list) выдаёт список файлов в текущем каталоге. Две основные опции:

- -a – просмотр всех файлов, включая скрытые;
- -l – отображение более подробной информации.

Команда «rm» используется для удаления файлов.

```
rm <имя_файла>
```

У данной программы существует ряд параметров. Самые часто используемые:

- -i – запрос на удаление файла;
- -r – рекурсивное удаление (т.е. удаление, включая подкаталоги и скрытые файлы).

Пример использования команды:

```
rm -i ~/html/*.html
```

Удаляет все файлы html, в каталоге html.

Команды «mkdir» и «rmdir». Команда «mkdir» позволяет создать каталог, тогда как «rmdir» удаляет каталог, при условии, что он пуст.

```
mkdir <имя_каталога>  
rmdir <имя_каталога>
```

Команда «rmdir» часто заменяется командой «rm -rf», которая позволяет удалять каталоги, даже если они не пусты.

Команда less позволяет постранично просматривать текст.

```
less <имя_файла>
```

Крайне полезно просмотреть файл, перед тем как его редактировать. Для выхода нужно нажать «q».

Команда «grep» имеет много опций и предоставляет возможности поиска символьной строки в файле.

```
grep <шаблон_поиска> <файл>
```

Команда «ps» отображает список текущих процессов. Колонка команд указывает имя процесса, колонка PID (идентификатор процесса) - номер процесса (этот номер используется, для операций с процессом, например чтобы «убить» его командой «kill»).

```
ps <аргументы>
```

Аргументы:

- -u – предоставляет больше информации;
- -x – позволяет просмотреть те процессы, которые не принадлежат пользователю (такие как те, что были запущены во время процесса загрузки).

Команда «kill» используется, если программа перестала отвечать или зависла, чтобы её завершить.

```
kill <PID_номер>
```

Иногда необходимо будет использовать «kill -9 <PID\_number>» (когда обычная команда «kill» не даёт желательного эффекта). Номер PID выясняется при помощи команды «ps».

Команда «cat» – утилита, выводящая последовательно указанные файлы (или устройства), таким образом объединяя их в единый поток. Если вместо имени файла указывается «-», то читается стандартный ввод.

```
cat <имя_файла>
```

Команда «sort» – утилита для вывода текстовых строк в определённом порядке.

```
sort <опции> <файл>
```

### 3.3 Использование многозадачности

РЕД ОС - это многозадачная система. Продемонстрируем на двух примерах, как это можно использовать.

Первый пример - запуск программы в фоновом режиме. Для того чтобы это сделать, вам нужно набрать «&» после имени программы. После этого оболочка даёт возможность запускать другие приложения. Пользователь должен быть внимательным, так как некоторые программы интерактивны, и их запуск в фоновом режиме не имеет смысла (подобные программы просто останутся, будучи запущенными в фоновом режиме). Для того, чтобы вернуть их в обычный режим, наберите:

```
fg <имя_программы>
```

Второй метод представляет собой запуск нескольких независимых сеансов. В консоли, нажмите «Ctrl + Alt» и одну из клавиш, находящихся в интервале от «F1» до «F6». На экране появится новое приглашение системы, и вы сможете открыть новый сеанс. Этот метод также позволяет вам работать на другой консоли, если консоль, которую вы использовали до этого, не отвечает, или вам необходимо остановить зависшую программу.

## 3.4 Режимы работы ОС

### 3.4.1 Диагностические режимы работы

С точки зрения функционирования ОС можно выделить 3 режима: нормальный (штатный), аварийный и режим восстановления.

Обычно ОС нормально функционирует и выполняет возложенные на неё функции в нормальном режиме. В этом режиме пользователь получает ожидаемый отклик на свои действия от ОС (в этом разделе нормальный режим рассмотрен не будет, ему посвящены остальные разделы руководства). Однако в ряде случаев, если в работе системы возникают проблемы, ОС может выполнить загрузку в режиме восстановления или аварийном режиме с целью диагностики и исправления проблем.

#### Режим восстановления

Режим восстановления позволяет загрузить минимальное окружение ОС с дистрибутивного носителя вместо загрузки с жёсткого диска. Этот режим предусмотрен для восстановления в случае сбоя. В штатном режиме ОС использует файлы на жёстком диске компьютера для запуска программ, хранения информации и прочих операций.

Однако не исключены ситуации, когда не получается полностью запустить ОС, чтобы иметь возможность обращения к файлам на жёстком диске. В режиме восстановления можно получить доступ к файлам, даже если не удалось запустить ОС с этого диска.

Если у вас нет возможности загрузиться с дистрибутивного носителя, то перейти в режим восстановления можно, выполнив следующие действия:

1. Начните загрузку ПК и дождитесь появления меню GRUB. Нажмите клавишу «E» для редактирования параметров загрузки.
2. Добавьте в конец строки, начинающейся с «linux /boot/vmlinuz ...», следующую запись:

```
systemd.unit=rescue.target
```

Используйте сочетание клавиш «Ctrl+A» (для перехода в начало строки) и «Ctrl+E» (для перехода в конец строки).

3. Нажмите «Ctrl+X» для загрузки ОС с указанными параметрами.

Загрузив систему, необходимо будет ответить на несколько простых вопросов, в частности, выбрать используемый язык и расположение корректного образа восстановления.

Если вы выбрали образ восстановления, который не требует подключения к сети, будет предложено определить, хотите ли вы установить сетевое подключение. Подключение к сети рекомендуется, если, например, нужно скопировать файлы на другой компьютер или установить какие-то RPM-пакеты с общего сетевого ресурса.

В режиме восстановления будет выполнена попытка найти установку ОС и подключить ее в /mnt/sysimage. После этого вы сможете внести необходимые изменения. Нажмите «Продолжить». Также можно подключить файловые системы в режиме чтения вместо чтения-записи. Если это не удалось, нажмите

кнопку «Пропустить» для перехода в командную оболочку.

При выборе «Продолжить» система попытается подключить файловую систему в `/mnt/sysimage`. Если смонтировать раздел не удастся, появится сообщение. При выборе варианта «только для чтения» будет предпринята попытка подключения файловой системы в `/mnt/sysimage/` в режиме чтения. Если вы выберете «Пропустить», файловая система не будет подключена. Выберите «Пропустить», если считаете, что файловая система повреждена.

Как только система загрузится в режиме восстановления, на виртуальных консолях появится приглашение (используйте «`Ctrl+Alt+Fx`» для перехода в нужную консоль).

Даже если файловая система подключена, в режиме восстановления корневым разделом по умолчанию становится временный раздел, а не тот, что используется при работе в обычном режиме. Если файловая система была смонтирована успешно, можно сменить корневой раздел окружения режима восстановления на корневой раздел вашей файловой системы, выполнив команду:

```
chroot /mnt/sysimage
```

Это может пригодиться для выполнения команд, требующих, чтобы корневой раздел системы был подключен как `/` (таких как `grm`). Чтобы выйти из окружения `chroot`, выполните команду «`exit`».

При выборе «Пропустить» можно попытаться смонтировать раздел или логический том LVM2 вручную в режиме восстановления, создав каталог, к примеру, с именем `/foo`, и выполнив следующую команду:

```
mount -t ext4 /dev/mapper/VolGroup00-LogVol102 /foo
```

В приведённой выше команде `/foo` — созданный вами каталог, а `/dev/mapper/VolGroup00-LogVol102` — логический том LVM2, который вы хотите смонтировать. Если раздел имеет тип `ext2` или `ext3`, замените `ext4` на `ext2` или `ext3`.

Если вы не знаете названий всех физических разделов, для их просмотра используйте команду:

```
fdisk -l
```

Если вы не знаете названий всех ваших физических томов LVM2, логических томов и их групп, их можно узнать, выполнив следующие команды:

```
pvdisplay  
vgdisplay  
lvdisplay
```

В строке приглашения можно выполнить множество полезных команд, включая следующие:

```
ssh, scp и ping, если сеть запущена;  
dump и restore, если вы используете ленточные накопители;
```

```
parted и fdisk для управления разделами;  
rpm для установки и обновления программного обеспечения;  
vi для редактирования текстовых файлов.
```

После завершения работы с повреждённой системой, можно перезагружать ОС в нормальном режиме.

### Аварийный режим

В аварийном режиме система будет загружена с минимальным окружением. Корневая файловая система подключается в режиме чтения и почти ничего настраивать не надо. Основным преимуществом этого режима является то, что файлы `init` не загружаются. Если окружение `init` повреждено и не работает, вы все же можете смонтировать файловые системы, чтобы восстановить данные, которые были потеряны при переустановке.

Чтобы загрузиться в аварийном режиме, выполните следующие действия:

1. Начните загрузку ПК и дождитесь появления меню GRUB. Нажмите клавишу «E» для редактирования параметров загрузки.
2. Добавьте в конец строки, начинающейся с «`linux /boot/vmlinuz ...`», следующую запись:

```
systemd.unit=emergency.target
```

Используйте сочетание клавиш «`Ctrl+A`» (для перехода в начало строки) и «`Ctrl+E`» (для перехода в конец строки).

3. Нажмите «`Ctrl+X`» для загрузки ОС с указанными параметрами.

### 3.4.2 Режимы отображения информации

С точки зрения представления информации для пользователя можно выделить 2 режима работы ОС: графический и консольный.

Консолью называется совокупность основных устройств ввода информации в компьютер (клавиатура и мышь) и вывода информации (монитор). ОС работает с несколькими так называемыми виртуальными консолями, из которых в каждый момент времени только одна может быть связана с реальной (физической) консолью (то есть, является активной).

Некоторые из консолей представляют информацию только в текстовом виде с использованием экранных шрифтов в форматах видеосистемы компьютера — консольный режим работы. Такие консоли называются иногда ещё текстовыми. Сама ОС и основные автоматически запускаемые приложения (такие как командный процессор) используют в таких консолях интерфейс командной строки. Другие приложения (например, менеджер файлов Midnight Commander) могут использовать оконный интерфейс, выделение объектов и выбор в меню и списках при помощи мыши или клавиатуры и т.п.

Другие консоли (графические) представляют информацию в графическом виде, используя Графический пользовательский интерфейс (GUI) — графический режим работы. Как правило, работа в таких консолях происходит при помощи развитых графических сред, таких как МАТЕ.

Для нужд ОС консоли перенумерованы целыми положительными числами

ми. Их общее количество может изменяться в зависимости от настроек ОС. Несколько первых консолей - текстовые, далее идут графические (в стандартной настройке - одна).

Если Вы работаете в графической консоли, для того чтобы сделать активной другую консоль с номером  $n$  (где  $n$  находится в интервале от 1 до 12), нажмите на клавиши «Ctrl+Alt+Fn», то есть, например клавиши «Ctrl+Alt+F2», если хотите перейти в консоль с номером 2. Для того чтобы сделать активной другую консоль вместо текущей текстовой консоли, нажмите на клавиши «Alt+Fn».

# Установка РЕД ОС

## 4. Установка РЕД ОС

### 4.1 Начало установки

Для начала установки, необходимо настроить BIOS СВТ, на которое производится установка РЕД ОС, на загрузку с оптического носителя информации (DVD-диска), на котором записан дистрибутив. Для этого необходимо включить в BIOS СВТ опцию загрузки с CD/DVD-привода. Способ входа в меню BIOS и расположение конкретных настроек может сильно отличаться, в зависимости от используемой материнской платы оборудования СВТ. Чаще всего для входа в BIOS необходимо нажать функциональную клавишу «Delete» на стационарных СВТ или функциональную клавишу «F1» («F9») на мобильных СВТ (ноутбуках), в момент начала загрузки компьютера. Для получения более подробных сведений по настройке необходимо обратиться к документации на используемое оборудование.

Загрузка с установочного носителя начинается с меню (рисунок 4.1), в котором перечислено несколько вариантов загрузки, причём установка системы - это только одна из возможностей. Из данного меню можно:

- запустить тестирование носителя данных и только после этого перейти к процедурам установке ОС;
- используя меню «Решение проблем», запустить проверку памяти и диагностику оборудования;
- запустить уже установленную ОС на жёстком диске;
- загрузить ОС в аварийном режиме.

Манипулятор графической информации (мышь) на этом этапе установки не поддерживается, поэтому для выбора различных вариантов и опций установки необходимо воспользоваться функциональными клавишами клавиатуры - стрелками. Можно скорректировать параметры запуска любого пункта начального меню установки РЕД ОС, нажав функциональную клавишу клавиатуры «TAB».

Кроме установки с оптического носителя информации доступно несколько вариантов сетевой установки и установка с флеш-диска.

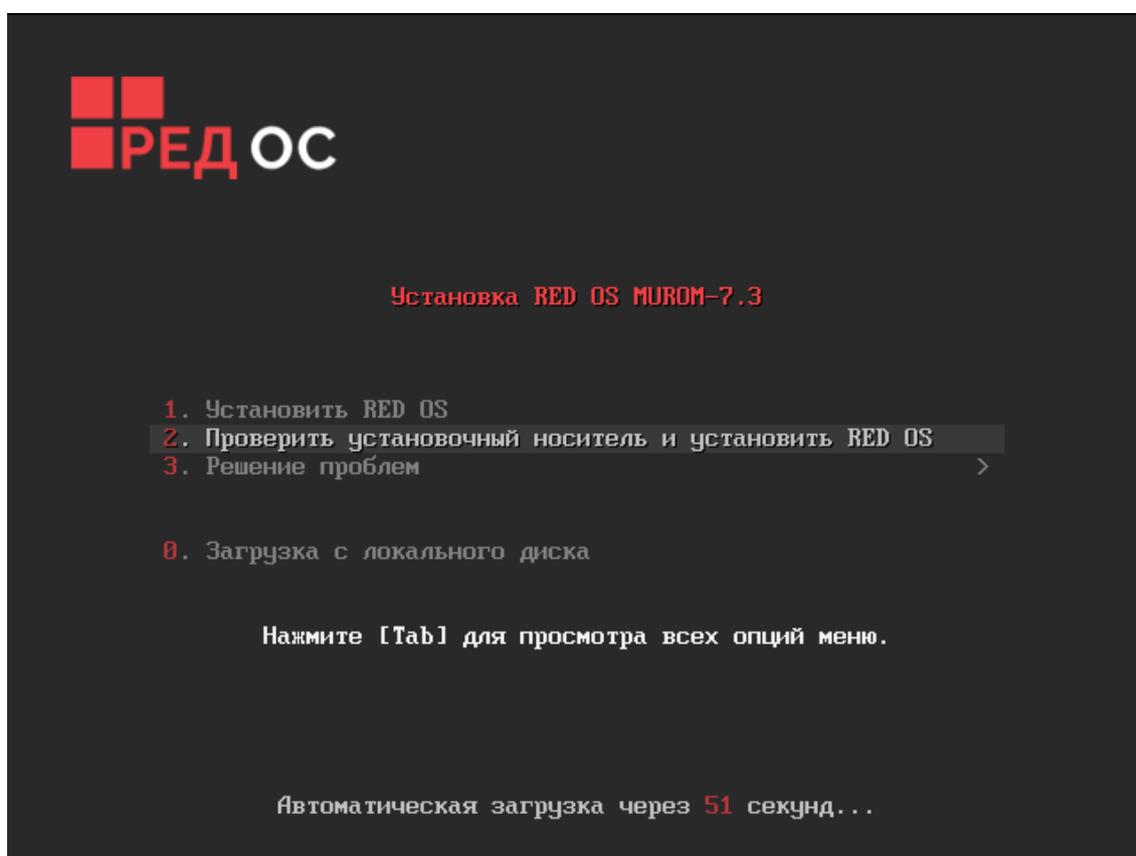


Рисунок 4.1 – Начальное меню установки РЕД ОС

Установка РЕД ОС автоматически осуществляется в графическом режиме с выводом текстовой информации на русском языке. Выбор языка установки РЕД ОС не осуществляется.

По умолчанию при установке используется графический видеорежим (разрешение экрана) 800 на 600 точек на дюйм. При возникновении проблем запуска установки в графическом режиме необходимо перезагрузить СВТ и повторить действия по установке, но с выбором в начальном меню установки с обычным видеодрайвером.

Чтобы начать процесс установки, нужно клавишами перемещения курсора «вверх», «вниз» выбрать пункт меню «Установить Red OS» и нажать «Enter». В начальном загрузчике установлено небольшое время ожидания продолжительностью 1 минута. Если в этот момент не предпринимать никаких действий, то будет загружена та система, которая уже установлена на жёстком диске. Если пропущен нужный момент, нужно перезагрузить компьютер и до истечения установленного времени ожидания выбрать нужный пункт в меню загрузчика.

Начальный этап установки не требует вмешательства пользователя: происходит автоматическое определение оборудования и запуск компонентов программы установки. Прервать начальный этап установки и вернуться в начальное меню установки РЕД ОС можно нажав клавишу «ESC».

Необходимость загрузиться в аварийном режиме может возникнуть в следующих случаях:

- невозможно загрузить ОС обычным образом;
- возникли программные или аппаратные проблемы и необходимо извлечь важные файлы с жёсткого диска.

Режим восстановления позволяет загрузить минимальное окружение ОС с дистрибутивного носителя вместо загрузки с жёсткого диска. В режиме восстановления можно получить доступ к файлам, даже если не удалось запустить ОС с этого диска.

В режиме восстановления будет выполнена попытка найти установку ОС и подключить ее в `/mnt/sysimage`. После этого можно будет внести необходимые изменения. Также можно подключить файловые системы в режиме чтения вместо чтения-записи.

В режиме восстановления также имеется возможность исправить работу загрузчика GRUB, который мог быть по ошибке удалён, повреждён или замещён загрузчиком другой операционной системы.

В ОС помимо режима восстановления есть аварийный режим. Режим восстановления эквивалентен однопользовательскому режиму и требует пароль `root`. Режим восстановления позволяет восстанавливать систему в ситуациях, когда она не может завершить обычный процесс загрузки. Режим восстановления попытается подключить все локальные файловые системы и запустить некоторые важные системные службы, но он не активирует сетевые интерфейсы и не разрешает вход в систему нескольким пользователям.

Аварийный режим обеспечивает минимальную возможную окружающую среду и позволяет восстанавливать систему даже в ситуациях, когда система не может войти в режим восстановления. В аварийном режиме система монтирует корневую файловую систему как доступную только для чтения, не пытается монтировать другие локальные файловые системы и не активирует сетевые интерфейсы.

## 4.2 Альтернативные способы установки

Для штатной установки дистрибутива РЕД ОС используется загрузочный оптический носитель информации - DVD-диск из комплекта поставки дистрибутива РЕД ОС. Если производится установка с такого диска, можно пропустить этот раздел и сразу перейти к следующему разделу.

Установка с оптического носителя информации (DVD-диска) - это лишь один из возможных способов установки РЕД ОС. Он подходит для большинства случаев, но не работает, например, в случае отсутствия на компьютере накопителя на оптических носителях информации - DVD-привода. Для таких случаев поддерживаются альтернативные методы установки. Важно понимать, что для начала установки необходимо две вещи: иметь возможность загрузить компьютер и иметь доступ к установочным файлам. В случае установочного дистрибутивного DVD-диска эти две возможности предоставляются самим диском: он является загрузочным и содержит все необходимые для установки файлы. Однако вполне допустим и такой вариант: первоначальная загрузка происходит

со специально подготовленного flash-диска, а установочные файлы берутся с FTP-сервера сети.

Таким образом, для установки дистрибутива необходимо:

- выбрать способ первоначальной загрузки компьютера;
- выбрать источник установки.

Для загрузки компьютера с целью установки операционной системы необходимо воспользоваться носителем, содержащим начальный загрузчик. Таким носителем может быть как сам загрузочный оптический диск, так и, например, flash-накопитель, который можно сделать загрузочным, воспользовавшись утилитой **iso2usb**.

### 4.2.1 Источники установки

После первоначальной загрузки с одного из поддерживаемых носителей, можно выбрать источник установки - место, откуда программа установки будет брать все необходимые при установке данные (прежде всего, устанавливаемое ПО). Так как установка системы возможна не только с лазерного диска, то можно выбрать один из поддерживаемых альтернативных источников установки.

Источники установки:

- Сетевые:
  - FTP-сервер;
  - NFS-сервер;
  - HTTP-сервер.
- Локальные:
  - Загрузочный флеш-диск.

Условием для всех способов установки является доступность дерева файлов, аналогичного содержимому установочного диска.

### 4.2.2 Запуск сетевой установки

Перед запуском сетевой установки производится настройка на сервере сети. Выполняется установка и настройка сервера DHCP.

```
dnf install dhcp
```

В файл конфигурации `/etc/dhcp/dhcpd.conf` вносятся следующие конфигурации:

```
subnet 10.YY.XX.0 netmask 255.255.255.0
{# диапазон ip-адресов организации
option subnet-mask 255.255.255.0;
option routers 10.YY.XX.1;
option broadcast-address 10.YY.XX.255;
option netbios-name-servers 10.YY.0.251;
option netbios-dd-server 10.YY.0.251;
option domain-name-servers 8.8.8.8;
option broadcast-address 10.YY.XX.255;
range 10.YY.XX.20 10.YY.XX.201;
```

```
}
default-lease-time 600;
max-lease-time 7200;
allow booting;
allow bootp;
option option-128 code 128 = string;
option option-129 code 129 = text;
next-server 10.YY.XX.1;
filename "/pxelinux.0";
```

Далее выполняется запуск сервиса:

```
service dhcpd start
```

Выполняется установка и настройка tftp-сервера.

```
dnf install tftp-server
```

В файл конфигурации `/etc/xinetd.d/tftp` вносятся следующие конфигурации:

```
disable = yes на disable = no
```

Выполняем перезапуск xinetd:

```
service xinetd restart
```

Выполняем подготовку необходимых файлов для начальной загрузки. Для этого устанавливаем утилиту syslinux.

```
dnf install syslinux
```

Копируем необходимые файлы в корневую директорию tftp-сервера:

```
cp /usr/share/syslinux/chain32.c32 /var/lib/tftpboot
cp /usr/share/syslinux/mboot.c32 /var/lib/tftpboot
cp /usr/share/syslinux/memdisk /var/lib/tftpboot
cp /usr/share/syslinux/menu.c32 /var/lib/tftpboot
cp /usr/share/syslinux/pxelinux.0 /var/lib/tftpboot
```

Создаём директории для конфигурации и дистрибутивов:

```
mkdir -p /var/lib/tftpboot/images/REDOS
mkdir -p /var/lib/tftpboot/pxelinux.cfg
```

Создаем файл меню `/var/lib/tftpboot/pxelinux.cfg/default` с содержимым:

```
default menu.c32
prompt 0
```

```
timeout 30
ONTIMEOUT local
MENU TITLE PXE Menu
LABEL REDOS
MENU LABEL REDOS
KERNEL images/REDOS/x86_64/7.3/images/pxeboot/vmlinuz
APPEND initrd=images/REDOS/x86_64/7.3/images/pxeboot/initrd.img
ramdisk_size=128000 ip=dhcp method=http://10.YY.X.1/images/REDOS/
/x86_64/7.3/ devfs=nomount
LABEL REDOS 7 i686
MENU LABEL REDOS 7.3 i686
KERNEL images/REDOS/i686/7.3/images/pxeboot/vmlinuz
APPEND initrd=images/REDOS/images/pxeboot/initrd.img ramdisk_size=
=128000 ip=dhcp method=http://10.YY.X.1/images/REDOS/ devfs=
nomount
```

Производим подготовку дистрибутивов РЕД ОС распаковкой содержимого установочных дисков РЕД ОС в соответствующие каталоги.

Для x86\_64 архитектуры:

```
mount -t iso9660 -o loop REDOS-DVD1.iso /iso
cp -vR /iso/ /var/lib/tftpboot/images/REDOS/
umount /iso
```

Производим установку web-сервера для обеспечения раздачи установочных образов:

```
dnf install lighttpd
```

В файл конфигурации /etc/lighttpd/lighttpd.conf вносятся следующие изменения:

```
var.server_root = "/var/lib/tftpboot"
server.use-ipv6 = "disable"
server.bind = "10.YY.X.1"
server.document-root = server_root
```

Производим запуск web-сервера:

```
service lighttpd start
```

Производится подготовка к сетевой установке РЕД ОС на рабочей станции. При сетевой установке со стороны клиента (компьютера, на который производится установка) необходимо определить параметры соединения с сервером установки. В этом случае на экране будут появляться диалоги, например, с предложением выбрать сетевую карту (если их несколько) или указать тип IP-адреса: статический (потребуется вписать его самостоятельно) или динамический (DHCP).

Для установки РЕД ОС на рабочей станции в BIOS СВТ выбираем загрузка

по сети: «Network Boot Agent» или «PXE boot». Конфигурирование выполняется в соответствии с технической документацией на конкретное оборудование СВТ рабочей станции. После конфигурирования производится перезагрузка СВТ и выполняется установка согласно штатной процедуре установки.

После успешного соединения с сервером в память компьютера будет загружен образ установочного диска, после чего начнётся установка системы так же, как и при установке с дистрибутивного DVD-диска.

### 4.3 Последовательность установки

До того, как будет произведена установка РЕД ОС на жёсткий диск СВТ, программа установки работает с образом системы, загруженным в оперативную память компьютера.

Если инициализация оборудования СВТ завершилась успешно, будет запущен псевдографический интерфейс программы-установщика (anaconda). Процесс установки реализован в виде «мастера» установки, который представляет собой интерактивный графический интерфейс, в котором пользователю предлагается отвечать на вопросы и указывать необходимые опции РЕД ОС. Мастер установки разделен на шаги, каждый шаг посвящён настройке или установке определённого сервиса системы. Шаги нужно проходить последовательно, переход к следующему шагу происходит по нажатию кнопки «Далее». При помощи кнопки «Назад» при необходимости можно вернуться к уже пройденному шагу и изменить настройки. На некоторых этапах установки возможность перехода к предыдущему шагу ограничена теми шагами, где нет зависимости от данных, введённых ранее.

Если по каким-то причинам возникла необходимость прекратить установку, нажмите «Reset» на системном блоке компьютера.

**Важно!** Совершенно безопасно прекращать установку только до шага «Подготовка диска», поскольку до этого момента не производится никаких изменений на жёстком диске. Если прервать установку между шагами «Подготовка диска» и «Установка загрузчика», вероятно, что после этого с жёсткого диска не сможет загрузиться ни одна из установленных систем. ■

Технические сведения о ходе установки можно посмотреть, нажав сочетание клавиш «Ctrl+Alt+F1», вернуться к программе установки - «Ctrl+Alt+F7». По нажатию «Ctrl+Alt+F2» откроется отладочная виртуальная консоль.

Во время установки РЕД ОС выполняются следующие шаги:

- выбор типа накопителя СВТ;
- присвоение имени компьютера в сети и настройка сетевых интерфейсов;
- выбор часового пояса;
- задание пароля администратора системы;
- подготовка разделов диска;
- выбор типа установки: сервер или рабочая станция;
- установка системы;
- установка загрузчика;

- перезагрузка системы;
- лицензионный договор;
- создание системного пользователя;
- установка даты и времени;
- сохранение настроек;
- завершение установки.

## 4.4 Язык

Язык интерфейса программы установки и графического интерфейса устанавливаемой РЕД ОС по умолчанию – русский, не конфигурируется и не изменяется в процессе установки. Дополнительным языком РЕД ОС является английский язык. Другие дополнительные языковые пакеты можно установить из репозитория после завершения установки РЕД ОС.

Переключение раскладки клавиатуры при установке РЕД ОС и в графическом интерфейсе РЕД ОС выполняется нажатием комбинации функциональных клавиш «Shift+Alt».

## 4.5 Обзор установки

После выбора языка необходимо произвести первоначальную конфигурацию установщика и параметров будущей системы (рисунок 4.2).

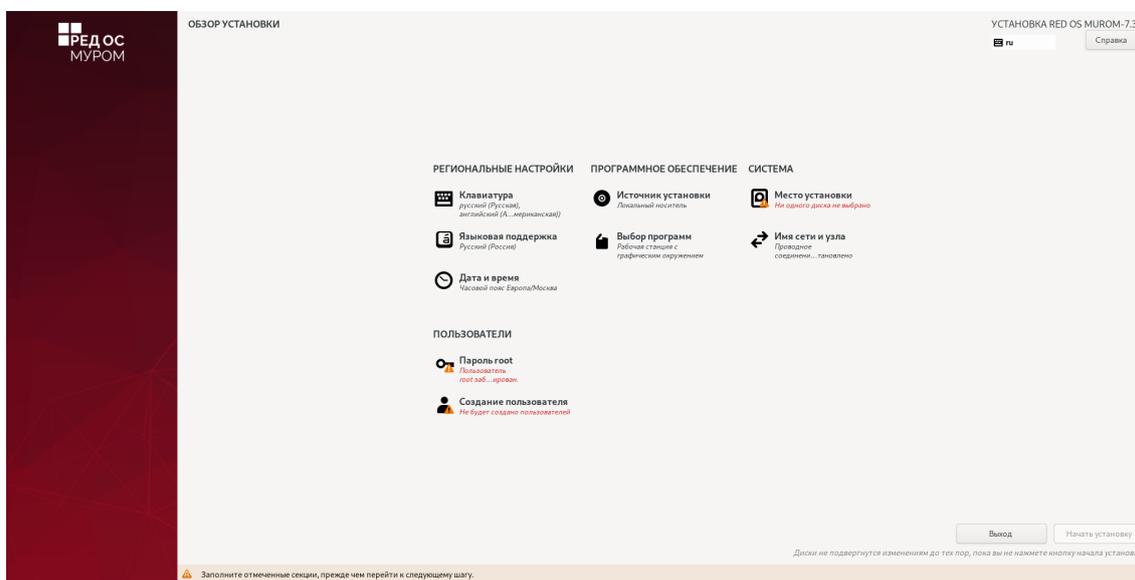


Рисунок 4.2 — Обзор установки

В этом окне необходимо задать региональные настройки, состав программного обеспечения и системные настройки. Здесь и в последующих окнах установщика красным цветом выводятся подсказки у тех вкладок, которые должны быть обязательно заполнены до перехода к следующему шагу установки.

Рассмотрим подробнее каждую вкладку окна.

### Дата и время

В окне настройки даты и времени (рисунок 4.3) можно выбрать текущий регион и город и установить используемое локальное время, дату и формат времени.

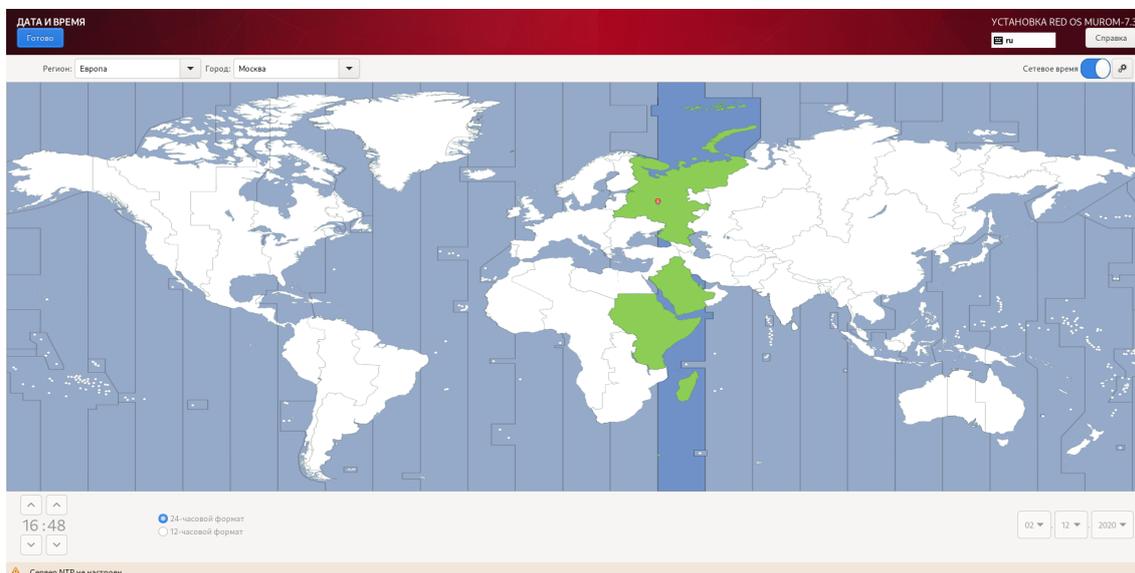


Рисунок 4.3 — Дата и время

Если установлена сеть, и есть доступ к глобальной сети, можно разрешить автоматическую настройку времени с помощью службы **ntp** — сетевое время.

Данную настройку можно изменить после завершения установки РЕД ОС. По умолчанию устанавливается часовой пояс UTC+03:00 (Европа/Москва).

Здесь и далее возврат в предыдущее меню осуществляется с помощью кнопки «Готово».

### Клавиатура

В окне настройки клавиатуры (рисунок 4.4) можно выбрать используемые в ОС раскладки.

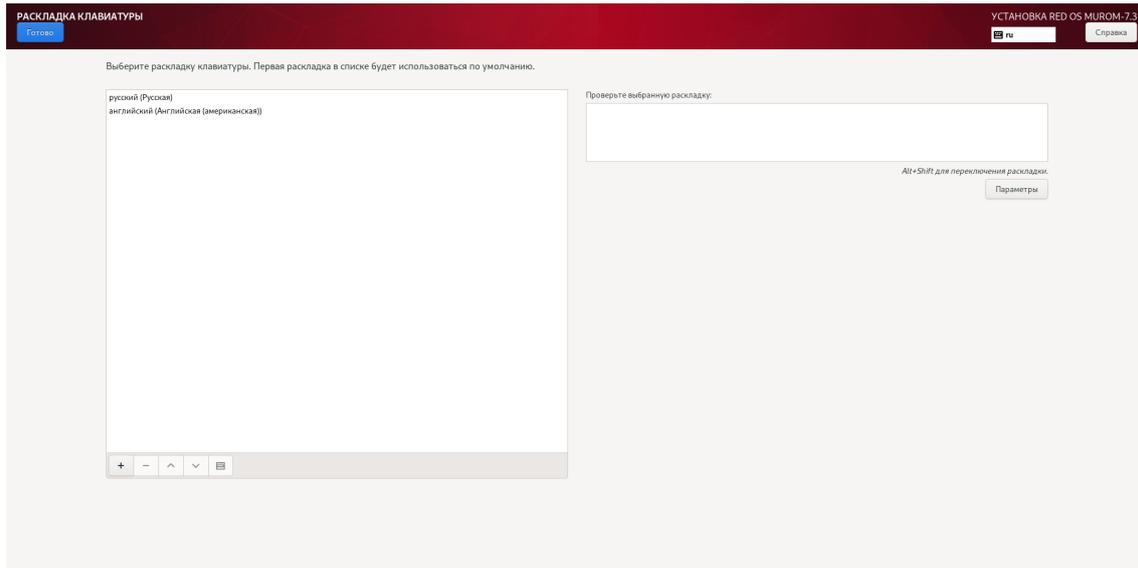


Рисунок 4.4 — Раскладка клавиатуры

В отдельном поле ввода можно проверить корректность отображения вводимых символов.

Первая раскладка в списке будет использоваться по умолчанию.

### Языковая поддержка

В окне языковой поддержки (рисунок 4.5) можно задать языки, которые будут установлены в системе. Настройка и выбор соответствующего языка будут доступны в настройках системы после установки. Также после установки системы можно будет добавить дополнительные языки, которые не были установлены ранее. По умолчанию используется русский язык интерфейса.

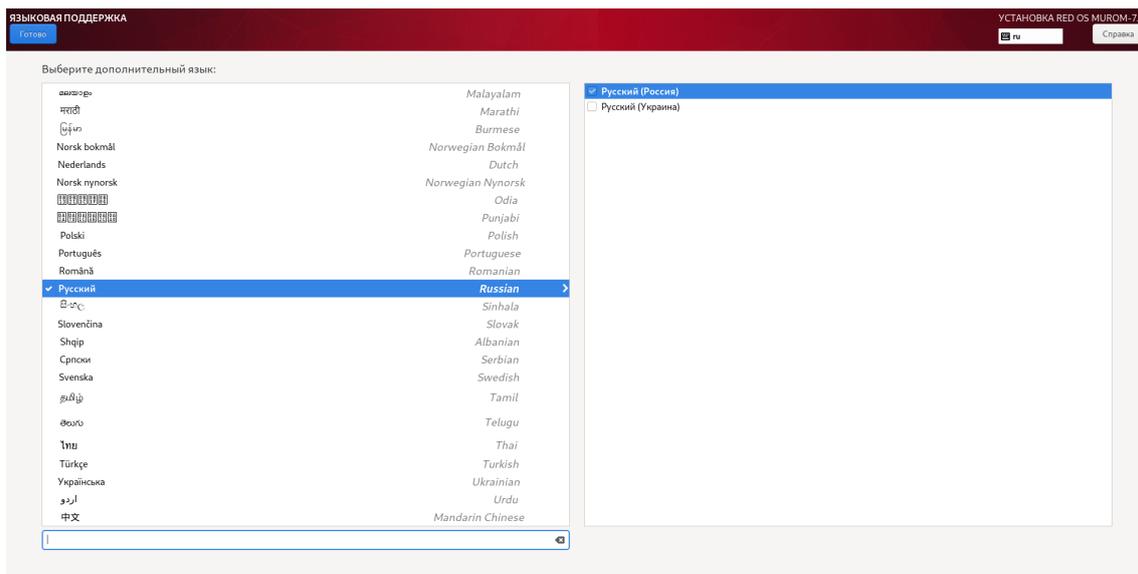


Рисунок 4.5 — Языковая поддержка

### Источник установки

В меню выбора источников установки (рисунок 4.6) можно задать, откуда система будет получать пакеты в процессе установки.

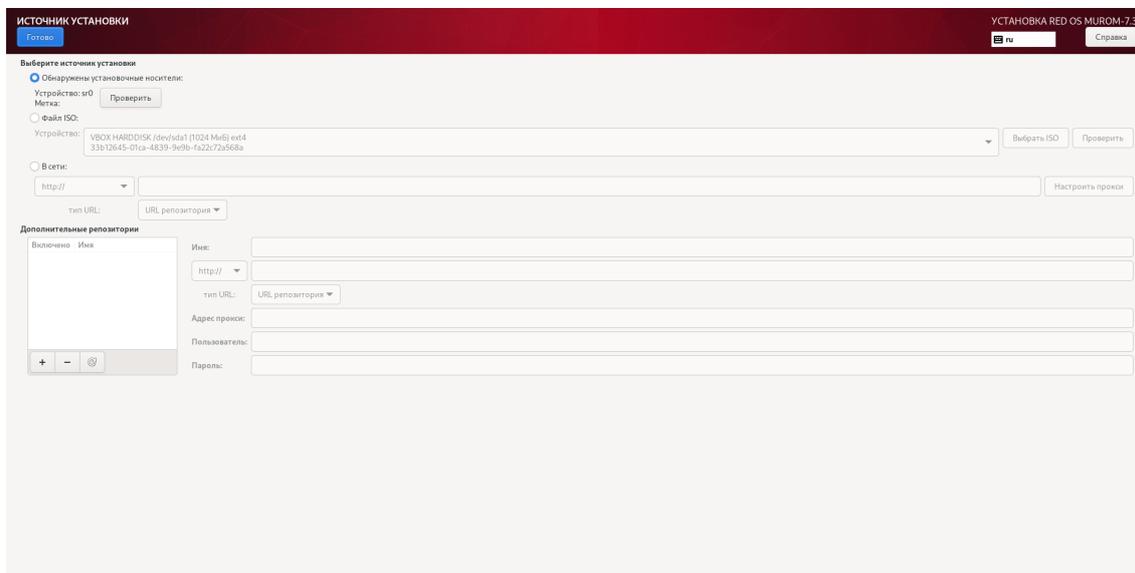


Рисунок 4.6 — Источник установки

Источниками установки могут быть локальные носители или сетевые источники.

### Выбор программ

В меню выбора программ (рисунок 4.7) можно задать, какая конфигурация из числа базового окружения будет установлена:

- рабочая станция;
- сервер минимальный;
- сервер с графическим интерфейсом.

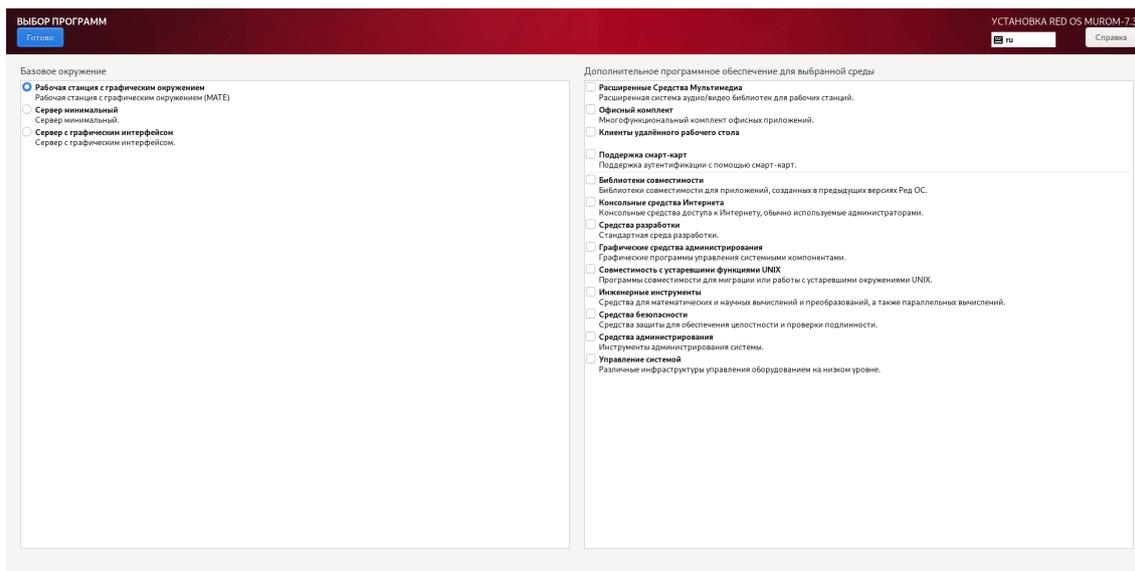


Рисунок 4.7 — Выбор программ

Дополнительно для каждой из выбранных конфигураций можно настроить группы пакетов, которые будут установлены.

В РЕД ОС все операции установки и удаления производятся над пакетами - отдельными компонентами системы. Пакет и программа соотносятся неоднозначно: иногда одна программа состоит из нескольких пакетов, иногда один пакет включает несколько программ.

В процессе установки РЕД ОС обычно не требуется детализированный выбор компонентов на уровне пакетов - это требует слишком много времени и знаний от проводящего установку. Тем более, что комплектация дистрибутива подбирается таким образом, чтобы из имеющихся программ можно было составить полноценную рабочую среду для соответствующей аудитории пользователей. Поэтому в процессе установки РЕД ОС пользователю предлагается выбрать из небольшого списка конфигураций, объединяющих пакеты, необходимые для решения наиболее распространённых задач.

### Расположение установки

В меню выбора расположения установки (рисунок 4.8) можно выбрать устройство для установки операционной системы.

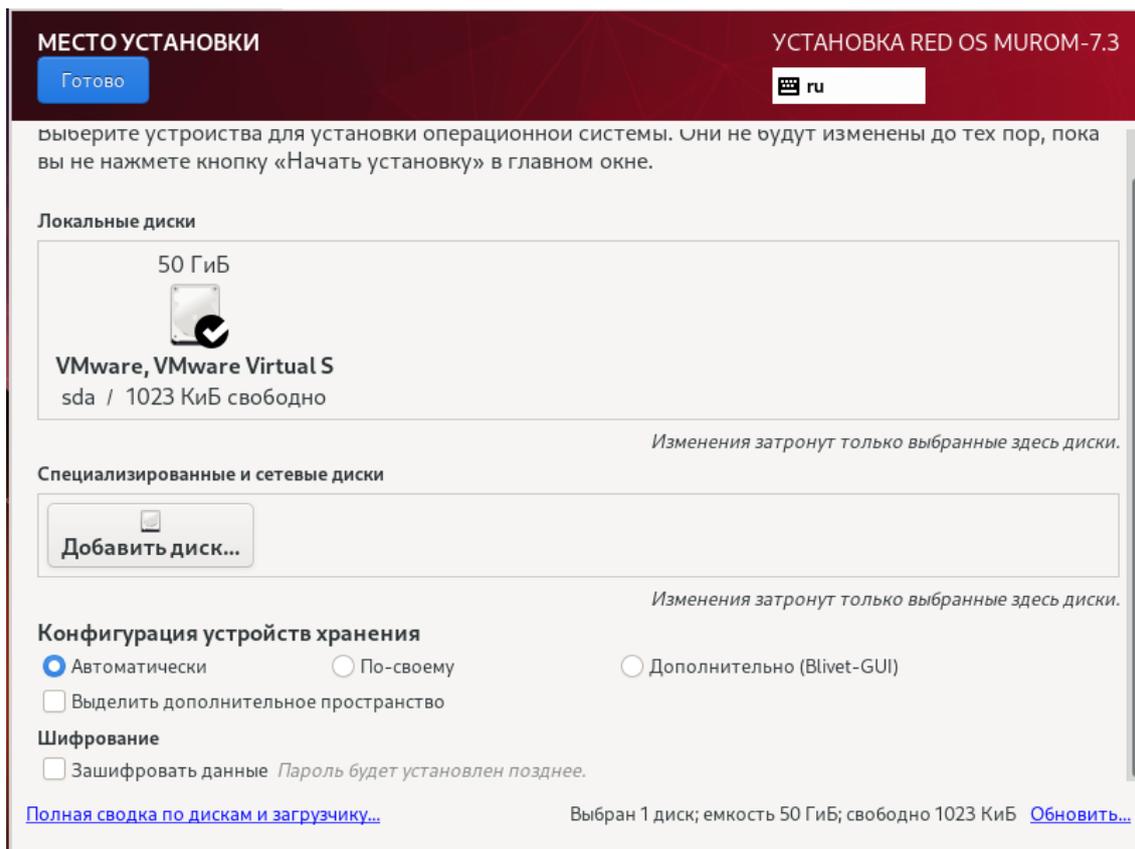


Рисунок 4.8 — Расположение установки

Переход к этому шагу может занять некоторое время. Время ожидания может быть разным и зависит от производительности компьютера, объёма и типов используемых накопителей, количества существующих разделов на них.

На этом этапе подготавливается площадка для установки РЕД ОС, в первую очередь - выделяется свободное место на диске.

Можно выбрать и использовать профили разбиения диска. Профиль - это шаблон распределения места на диске для установки РЕД ОС.

Можно выбрать:

- автоматически;
- по-своему;
- дополнительно (Blivet-GUI).

Первый профиль предполагает автоматическое разбиение диска. Будет выбрано оптимальное расположение ОС.

Необратимые изменения разделов на жёстком диске требуют подтверждения со стороны пользователя. После подтверждения внесённые изменения сохраняются на жестком диске/дисках СВТ.

Если для применения одного из профилей автоматической разметки доступного места окажется недостаточно, будет выведено сообщение о невозможности выполнения операции разбиения диска.

При необходимости можно освободить часть дискового пространства, для этого следует воспользоваться профилем разбиения вручную. Можно удалить

некоторые из существующих разделов или содержащиеся в них файловые системы. После этого можно создать необходимые разделы самостоятельно или вернуться к шагу выбора профиля. Выбор этой возможности требует знаний об устройстве диска и технологиях его разбиения.

По нажатию «Готово» будет произведена запись новой таблицы разделов на диск и форматирование разделов. Разделы, только что созданные на диске программой установки, пока не содержат данных и поэтому формируются без предупреждения. Уже существовавшие, но изменённые разделы, которые будут отформатированы, помечаются специальным значком в колонке «Файловая система».

Не следует форматировать разделы с теми данными, которые необходимо сохранить, например, с пользовательскими данными (/home) или с другими операционными системами. С другой стороны, отформатировать можно любой раздел, который необходимо «очистить» (т.е. удалить все данные).

Blivet-gui является обособленной реализацией механизмов управления разделами и дисками, снабжённой привычным интерфейсом в стиле GParted. Программа поддерживает управление дисковыми разделами и хранилищами LVM2 (включая зашифрованные разделы LUKS, логические тома и группы томов). Так же как и в GParted, изменения в blivet-gui применяются не сразу, а после подтверждения внесённого набора изменений.

### Сеть и имя узла

В меню выбора настройки сети (рисунок 4.9) можно активировать соединение с сетью и задать имя узла.

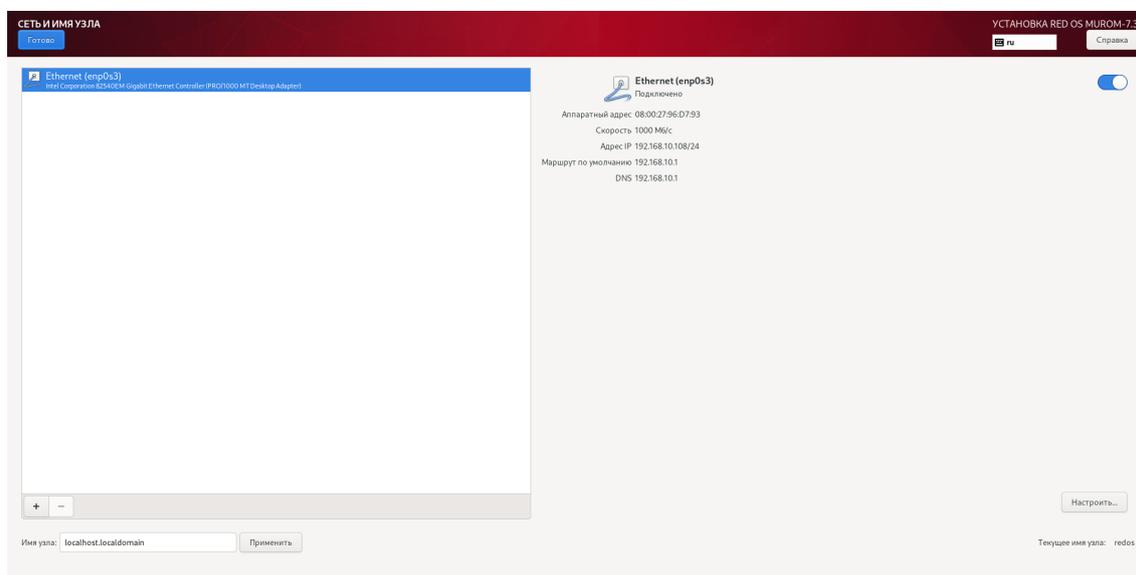


Рисунок 4.9 — Сеть и имя узла

На данном этапе необходимо задать имя компьютера в сети (хоста). При наличии сети имя компьютера используется для однозначного определения каждого компьютера. Имя компьютера состоит непосредственно из имени компьютера и

имени домена в сети, к которому принадлежит компьютер. Имя компьютера и имя домена разделяются знаком «.» .

При наличии домена сети имя должно даваться полностью. При отсутствии сети домену также может быть дано произвольное имя.

В качестве букв в имени компьютера разрешается использовать только буквы латиницы. В имени компьютера не допускается использование заглавных букв, пробелов и специальных символов.

Так же на данном этапе можно сконфигурировать параметры настройки сетевых интерфейсов: автоматическое включение интерфейсов, MAC-адреса сетевых интерфейсов, параметры сетевых протоколов.

## 4.6 Задание пароля администратора системы

После того как предварительная настройка системы завершена, начинается непосредственная установка системы. Параллельно с установкой необходимо настроить пароль администратора root и при необходимости создать учётные записи пользователей (рисунок 4.10)

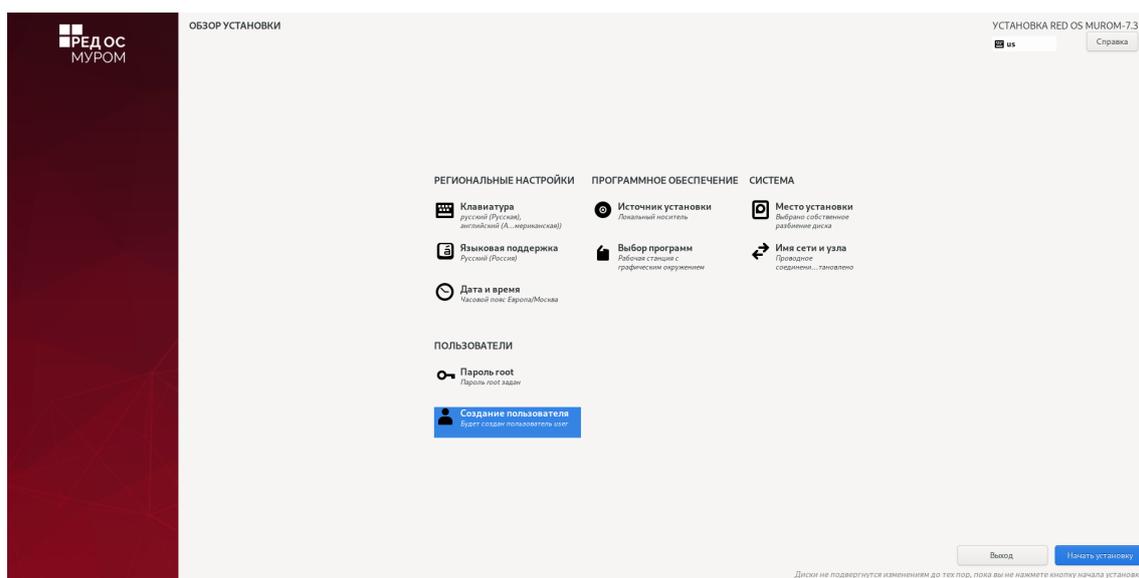


Рисунок 4.10 — Конфигурация ОС

РЕД ОС - это многопользовательская операционная система. На практике это означает, что для работы в системе нужно в ней зарегистрироваться, т.е. дать понять системе, кто именно находится за монитором и клавиатурой. Наиболее распространённый способ регистрации на сегодняшний день - использование системных имён (login name) и паролей. Это надёжное средство убедиться, что с системой работает тот, кто нужно, если пользователи хранят свои пароли в секрете и если пароль достаточно сложен и не слишком короток (иначе его легко угадать или подобрать).

В ОС всегда присутствует один специальный пользователь - администратор, он же суперпользователь или администратор РЕД ОС, для него зарезервировано стандартное системное имя - root.

Необходимо запомнить пароль root - его нужно будет вводить, чтобы получить право изменять настройки системы с помощью стандартных средств настройки РЕД ОС (рисунок 4.11).

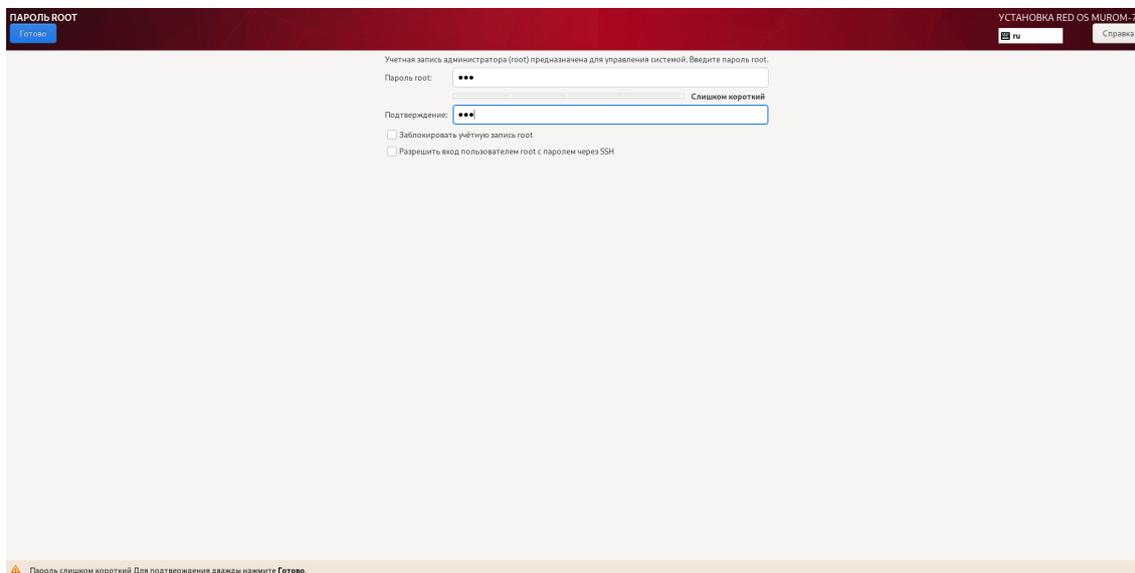


Рисунок 4.11 – Задание пароля администратора РЕД ОС

Ввод пароля защищён, при наборе пароля вместо символов на экране отображаются специальные символы. Чтобы избежать опечатки при вводе пароля, его предлагается ввести дважды. К введённому паролю в режиме реального времени применяется политика сложности пароля, т.е. производится его проверка, при слишком простом пароле или совпадении пароля с парольной последовательностью из словаря паролей системой будет предложено произвести смену пароля администратора РЕД ОС.

Администратор отличается от всех прочих пользователей тем, что ему позволено производить любые, в том числе самые разрушительные, изменения в системе. Поэтому выбор пароля администратора РЕД ОС - очень важный момент для безопасности: любой, кто сможет ввести его правильно (узнать или подобрать), получит неограниченный доступ к системе. Даже ваши собственные неосторожные действия от имени root могут иметь катастрофические последствия для всей системы.

Помимо администратора РЕД ОС (root) в систему необходимо добавить, по меньшей мере, одного обычного пользователя. Работа от имени администратора РЕД ОС считается опасной (можно по неосторожности повредить систему), поэтому повседневную работу в РЕД ОС следует выполнять от имени обычного пользователя, полномочия которого ограничены.

При добавлении пользователя предлагается ввести имя учётной записи (login name) пользователя. Имя учётной записи всегда представляет собой одно слово, состоящее только из строчных латинских букв (заглавные запрещены), цифр и символа подчёркивания «\_» (причём цифра и символ «\_» не могут стоять в начале слова). Чтобы исключить опечатки, пароль пользователя вводится дважды.

Так же, как при выборе пароля администратора РЕД ОС (root), действуют требования по сложности пароля.

В процессе установки предлагается создать только одну учётную запись обычного пользователя - чтобы от его имени системный администратор РЕД ОС мог выполнять задачи, которые не требуют привилегий суперпользователя.

Учётные записи для всех прочих пользователей системы можно будет создать в любой момент после её установки.

## 4.7 Установка системы

Этап установки происходит параллельно с заданием пароля администратора и представляет собой установку набора программ, необходимых для работы системы (рисунок 4.12).

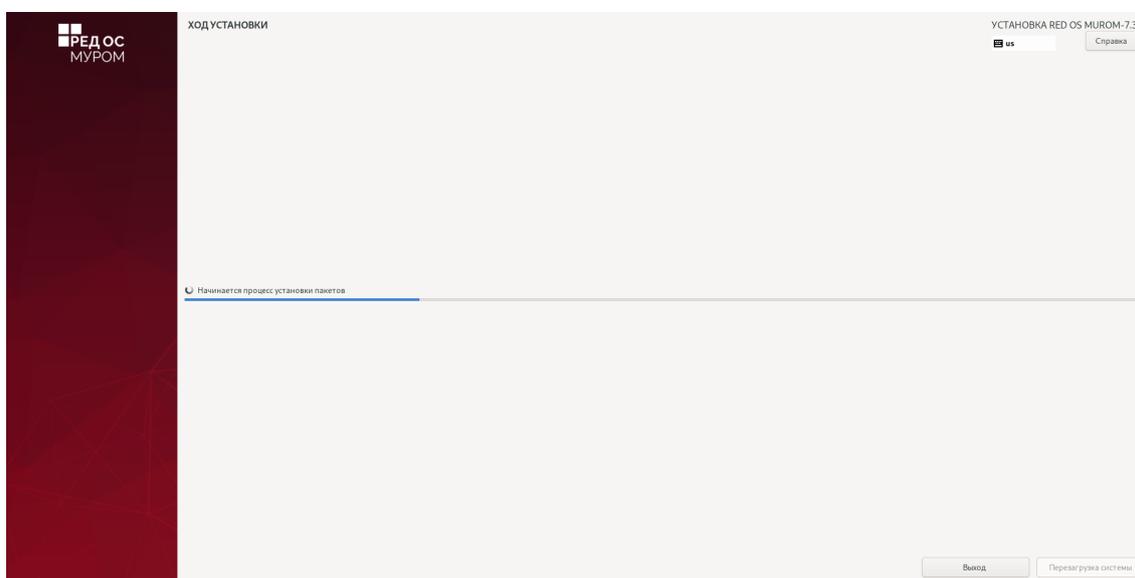


Рисунок 4.12 – Установка пакетов РЕД ОС

Получение пакетов осуществляется с источника, выбранного на этапе начальной загрузки. При сетевой установке (по протоколу FTP или HTTP) время выполнения этого шага будет зависеть от скорости соединения и может быть значительно большим, чем при установке с дистрибутивного DVD-диска.

Начиная с этого шага, программа установки работает с файлами только что установленной базовой системы. Все последующие изменения можно будет совершить после завершения установки посредством редактирования соответствующих конфигурационных файлов или при помощи модулей управления, включённых в дистрибутив.

Загрузчик — программа, которая позволяет загружать установленные операционные системы. При автоматическом разбиении разделов накопителя на жестких дисках средства вычислительной техники загрузчик автоматически устанавливается в начальный раздел диска.

Если же планируется использовать и другие операционные системы, уже установленные на этом компьютере, тогда имеет значение, на каком жёстком дис-

ке или разделе будет расположен загрузчик. В большинстве случаев программа установки правильно подберёт расположение загрузчика.

После выполнения копирования файлов РЕД ОС и установки загрузчика пользователю предлагается произвести перезагрузку РЕД ОС кнопкой «Перезагрузить».

#### 4.8 Соглашение пользователя и Лицензионный договор

После успешной перезагрузки и перед продолжением установки следует внимательно прочитать условия пользовательского соглашения (рисунок 4.13).

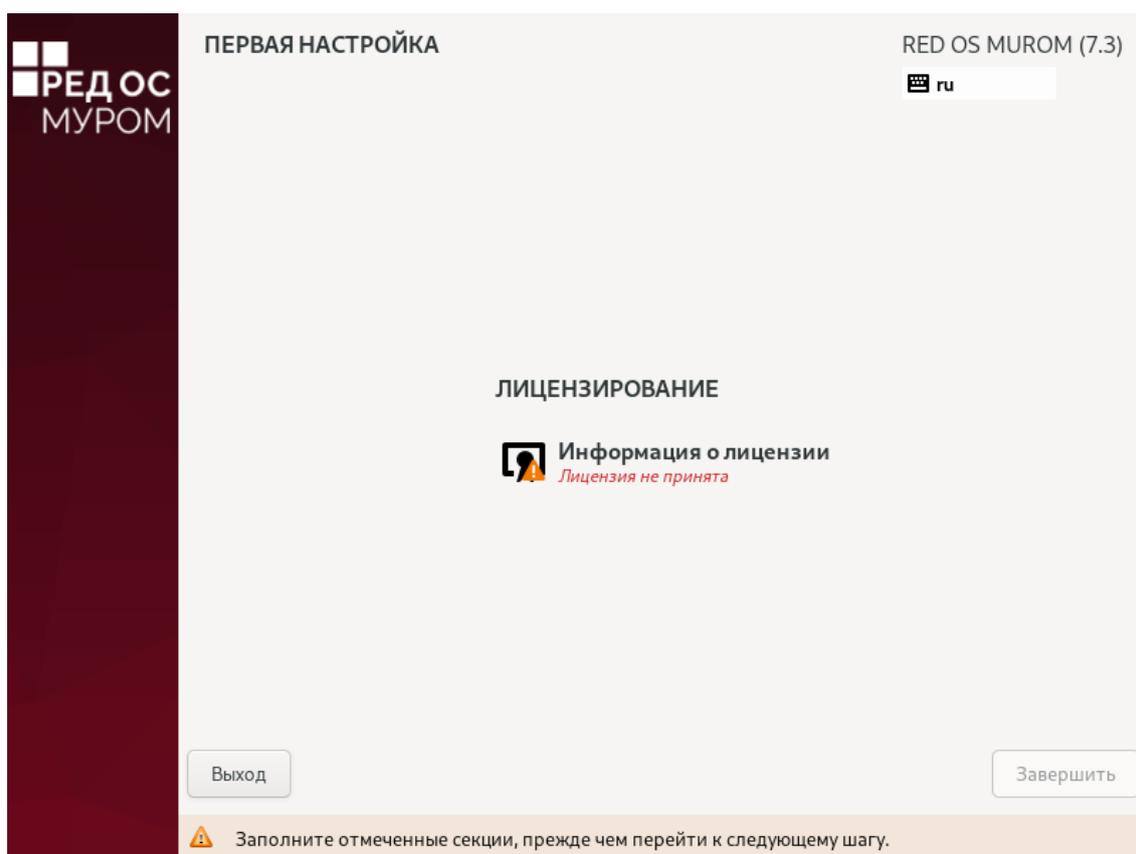


Рисунок 4.13 – Первая настройка

В лицензии (рисунок 4.14) говорится о правах распространения и гарантиях производителя.

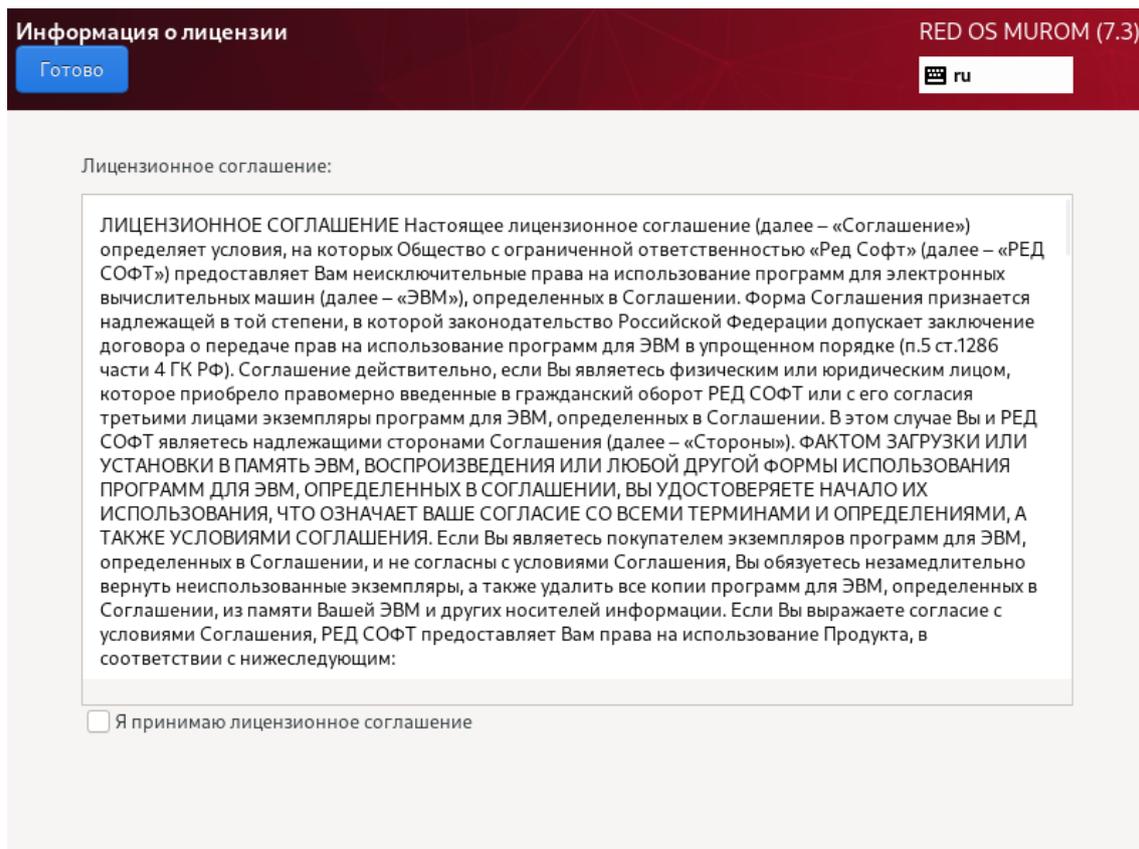


Рисунок 4.14 - Лицензия

При приобретении дистрибутива данное лицензионное соглашение прилагается в печатном виде к копии дистрибутива на вкладыше комплекта дистрибутива. Лицензия относится ко всему дистрибутиву РЕД ОС.

## 4.9 Завершение установки

После сохранения настроек и перезапуска системы пользователю предоставляется экран приветствия и приглашения к авторизации. На этом установка и настройка РЕД ОС завершена, и РЕД ОС полностью готова к использованию.

## 4.10 Подготовительные процедуры

После установки РЕД ОС не все функции безопасности включены по умолчанию. Администратор должен определить функциональную роль установленной копии ОС, перечень решаемых задач, и в соответствии с действующими политиками безопасности организации и роли пользователя, который планирует использовать ОС, произвести активацию необходимых служб, сервисов и приложений. А именно:

- сконфигурировать перечень отслеживаемых событий безопасности (принимая во внимание то, что журналы аудита при отслеживании всех системных событий могут иметь огромный размер и быстро исчерпать свободное место

- на жёстком диске, по умолчанию в ОС включено отслеживание лишь определённого числа критически важных событий; как настроить необходимые в данный момент события см. в разделе «Аудит в РЕД ОС»);
- настроить действия в случае обнаружения критически важных событий безопасности (см. раздел «Аудит в РЕД ОС»);
  - настроить действия для предотвращения потери данных аудита (см. описание конфигурационного файла `auditd.conf`);
  - создать необходимое количество пользователей, групп, ролей и связать пользователей с группами и ролями, исходя из необходимых им полномочий (см. подразделы «Управление пользователями», «SELinux»);
  - установить права доступа на создаваемые вновь каталоги и файлы (см. подраздел «Права доступа к файлам и каталогам»);
  - определить правила установки программ и правила запуска компонентов программного обеспечения (см. подраздел «Система управления пакетами DNF», «Systemd»);
  - определить и настроить используемые механизмы идентификации и аутентификации (по умолчанию используется простая парольная аутентификация и идентификация по логину пользователя), сроки действия учётных записей и паролей, требования, предъявляемые к аутентификационным данным, задать для пользователей системы не более 4 неуспешных попыток аутентификации, после которых должна выполняться временная блокировка учётной записи пользователя (см. подраздел «PAM»);
  - создать необходимые резервные копии данных, аудита и системных настроек и проводить периодическое их тестирование (см. подразделы «Утилиты для работы с файловыми системами», «Crontab», «AMTU», «Экспорт данных пользователя», «Резервирование данных»);
  - настроить доверенные сервера точного времени (см. подраздел «ntpd»);
  - проверить целостность важных данных и системных файлов (см. подраздел «Afsck»);
  - организовать отказоустойчивый кластер при необходимости обеспечения пониженной отказоустойчивости (см. подраздел «Отказоустойчивый кластер»);
  - определить квоты и приоритеты, выделяемые пользователям (см. подразделы «Изменение приоритета процесса», «Управление дисковыми квотами», «Ограничение ресурсов пользователя»);
  - установить необходимые ограничения на сеансы пользователей (см. подраздел «PAM»);
  - установить продолжительность бездействия пользовательского сеанса, после которого сеанс будет заблокирован или завершён (см. подраздел «Настройка хранителя экрана, блокировки и режима энергосбережения» документа «Операционная система «РЕД ОС». Руководство пользователя»).

Информация, приведённая в данном руководстве, должна использоваться совместно со встроенной справочной системой `man`.

# Управление программным обеспечением

## 5. Управление ПО

### 5.1 Введение: пакеты, зависимости и репозитории

В РЕД ОС огромное число общих ресурсов, которыми пользуются сразу несколько программ: разделяемых библиотек, содержащих стандартные функции, исполняемых файлов, сценариев и стандартных утилит и т.д. Удаление или изменение версии одного из составляющих систему компонентов может повлечь неработоспособность других, связанных с ним компонентов, или даже вывести из строя всю систему. В контексте системного администрирования проблемы такого рода называют нарушением целостности системы. Задача администратора - обеспечить наличие в системе согласованных версий всех необходимых программных компонентов (обеспечение целостности системы).

Для установки, удаления и обновления программ и поддержания целостности системы используются менеджеры пакетов. С точки зрения менеджера пакетов программное обеспечение представляет собой набор компонентов - программных пакетов. Такие компоненты содержат в себе набор исполняемых программ и вспомогательных файлов, необходимых для корректной работы программного обеспечения. Менеджеры пакетов облегчают установку программ: они позволяют проверить наличие необходимых для работы устанавливаемой программы компонент подходящей версии непосредственно в момент установки, а также производят необходимые процедуры для регистрации программы во всех операционных средах пользователя: сразу после установки программа может быть доступна пользователю из командной строки и - если это предусмотрено - появляется в меню всех графических оболочек.

**Важно!** Благодаря менеджерам пакетов, пользователю обычно не требуется непосредственно обращаться к установочным процедурам отдельных

программ или непосредственно работать с каталогами, в которых установлены исполняемые файлы и компоненты программ (обычно это `/usr/bin`, `/usr/share/<имя_пакета>`) - всю работу делает менеджер пакетов. Поэтому установку, обновление и удаление программ обычно называют управлением пакетами. ■

Часто компоненты, используемые различными программами, выделяют в отдельные пакеты и помечают, что для работы ПО, предоставляемого пакетом А, необходимо установить пакет В. В таком случае говорят, что пакет А зависит от пакета В или что между пакетами А и В существует зависимость.

Отслеживание зависимостей между такими пакетами представляет собой серьёзную задачу - некоторые компоненты могут быть взаимозаменяемыми: может обнаружиться несколько пакетов, предлагающих затребованный ресурс.

Задача контроля целостности и непротиворечивости установленного в системе ПО ещё сложнее. Представим, что некие программы А и В требуют наличия в системе компоненты С версии 1.0. Обновление версии пакета А, требующее обновления компоненты С до новой, использующей новый интерфейс доступа, версии (скажем, до версии 2.0), влечёт за собой обязательное обновление и программы В.

Однако менеджеры пакетов оказались неспособны предотвратить все возможные коллизии при установке или удалении программ, а тем более эффективно устранить нарушения целостности системы. Особенно сильно этот недостаток сказывается при обновлении систем из централизованного репозитория пакетов, в котором последние могут непрерывно обновляться, дробиться на более мелкие и т. п. Этот недостаток и стимулировал создание систем управления программными пакетами и поддержания целостности системы.

Для автоматизации этого процесса в РЕД ОС применяется система управления программными пакетами DNF.

## 5.2 Основы работы с RPM

RPM (Redhat Package Manager) служит для работы с пакетами - установка, удаление, проверка и т.д. При установке пакета `rpm` записывает информацию о нем в свою базу данных, что и позволяет в дальнейшем удалять пакет, просматривать информацию о нем и т.д.

Такой подход к установке ПО имеет несколько достоинств, в частности:

- унифицированная работа с разными пакетами;
- отслеживание зависимостей между пакетами выполняется автоматически;
- непротиворечивость между разными пакетами.

Если вызвать `rpm` без параметров, то он покажет краткий список ключей. Обычно же формат вызова `rpm` такой:

```
rpm -<ключ_режима> <дополнительные_ключи> <параметры>
```

<ключ\_режима>, указываемый первым, определяет режим работы.

Основные варианты вызова `rpm` приведены в таблице.

Команда	Описание команды
<code>rpm -i &lt;файл_пакета&gt;.rpm</code>	Установка пакета (install).
<code>rpm -U &lt;файл-пакета&gt;.rpm</code>	Обновление пакета (upgrade).
<code>rpm -e &lt;пакет&gt;</code>	Удаление пакета (erase).
<code>rpm -q &lt;пакет&gt;</code>	Получение информации (query).
<code>rpm -v &lt;пакет&gt;</code>	Проверка пакета (verify).
<code>rpm -b</code>	Создание пакета .rpm из .src.rpm (build).

В аргументах обычно используется два варианта ссылок на пакеты.

Имя <файла-пакета>.rpm для режимов «-i» и «-U» – это полное (с директорией) имя файла. Пример команды выглядит следующим образом:

```
~/RPMS/apache-1.3.3-1.i386.rpm
```

В принципе, rpm понимает имена файлов в виде ftp-URL, т.е.:

```
ftp://<сервер>/<директория>/<файл>.rpm
```

Пакет – это имя уже установленного пакета для режимов «-e», «-q» и «-u». Оно может указываться как с номером версии, так и без него.

Примеры:

```
acroread-3.01-4  
acroread
```

Если вместо списка пакетов указать ключ «-a» (all), то это будет означать «все пакеты». Кроме того, ключ «-f» позволяет вместо имени пакета указать какой-либо файл, принадлежащий этому пакету.

Можно указывать не один файл-пакета или пакет, а сразу несколько, разделяя их пробелами.

Команда «rpm -q» позволяет получать следующую информацию о пакете:

- версию пакета;
- список файлов;
- чего требует пакет;
- можно узнать, какому пакету принадлежит указанный файл.

Просто «rpm -q <имя-пакета>» выдаёт полное название пакета, вместе с версией. Но чаще всего команда «rpm -q» используется для получения списка файлов пакета.

Команда «rpm -qi» (info) выдаёт сводку информации о пакете – название, версию, объем и т.д., плюс краткую аннотацию.

Для получения списка файлов используется ключ «-l» (list).

Поскольку некоторые пакеты содержат очень большое количество файлов, то стоит отправлять вывод от «rpm -ql» команде «less».

Для получения «полной» информации о пакете (аннотации и списка файлов) можно указать ключи «-i» и «-l» одновременно.

Часто возникает необходимость узнать, какому пакету принадлежит какой-то файл (например, чтобы знать, где искать к нему документацию). Для этого можно воспользоваться ключом «-f» (file).

При этом надо указывать полное имя файла - с директорией. Кроме того, если к файлу есть «несколько путей» (из-за символических линков на директории), то следует указывать «основной» (обычно тот, который без символических линков), иначе `rpm` не сможет дать ответ.

Ключ «-R» (Requirements) позволяет узнать, какие пакеты и библиотеки требуются пакету. Особенно часто это требуется перед установкой пакета. Команда «`rpm -u`» пакет позволяет сравнить текущее состояние файлов пакета с информацией, записанной в базе данных. Это требуется, например, при проверке, не испорчены ли какие-нибудь важные для системы файлы (такое случается после внезапного отключения питания). При нахождении различий печатается ключевая строка, с обозначением отличий и имя файла, в котором они найдены.

### 5.3 Назначение DNF

Фактически, `dnf` представляет собой оболочку для `rpm`, обеспечивающую работу с репозиториями. Утилита `dnf` - это менеджер пакетов, который умеет запрашивать информацию о пакетах, получать пакеты из репозиториев, устанавливать и удалять их, используя автоматическое разрешение зависимостей, а также обновлять целиком систему до последних версий пакетов. DNF выполняет автоматическое разрешение зависимостей для пакетов, которые обновляются, устанавливаются или удаляются, и, таким образом, позволяет автоматически определять, получать и устанавливать все доступные по зависимостям пакеты. Для DNF можно настроить новые, дополнительные репозитории, или, по-другому, источники пакетов, кроме того, для него доступны многие дополнения, которые улучшают и расширяют его возможности. DNF позволяет выполнять многие из задач, которые выполняет RPM; кроме того, многие из опции командной строки у него также подобны опциям RPM. Утилита `dnf` обеспечивает простое и легкое управление пакетами на одной машине или же на группе машин.

DNF обеспечивает безопасное управление пакетами путем включения проверки сигнатур GPG для пакетов, подписанных с помощью GPG, для всех репозиториев пакетов или для отдельных репозиториев. В случае включения проверки сигнатур, DNF откажется устанавливать любые пакеты, не подписанные корректным ключом для данного репозитория. Это означает, что можно доверять пакетам RPM, которые скачиваются и устанавливаются на машине в том случае, если они получены из доверенных источников, и они не были изменены в процессе передачи.

DNF также позволяет легко создавать собственные репозитории RPM-пакетов для скачивания и установки их на других машинах.

## 5.4 Источники программ (репозитории)

Репозитории, с которыми работает DNF, отличаются от обычного набора пакетов наличием мета информации - индексов пакетов, содержащихся в репозитории, и сведений о них. Поэтому, чтобы получить всю информацию о репозитории, DNF достаточно получить его индексы.

DNF может работать с любым количеством репозиторий одновременно, формируя единую информационную базу обо всех содержащихся в них пакетах. При установке пакетов DNF обращает внимание только на название пакета, его версию и зависимости, а расположение в том или ином репозитории не имеет значения. Если потребуется, DNF в рамках одной операции установки группы пакетов может пользоваться несколькими репозиториями.

**Важно!** При использовании РЕД ОС (стандартной и сертифицированной редакции), в целях предотвращения нарушения целостности системы, **ЗАПРЕЩАЕТСЯ** настройка служб автоматического обновления на использование внешних сторонних репозиторий операционных систем.

Подключение репозитория сторонней ОС влечет за собой нарушение зависимостей в устанавливаемых пакетах. Принудительная установка пакетов из репозитория сторонней ОС может привести к неработоспособности как отдельных компонентов системы, так и ОС в целом.

Если для обеспечения рабочих процессов пользователя нужен пакет (программа, утилита), которого нет в РЕД ОС (и/или требуется обновление версий пакетов, которые уже есть в репозитории РЕД ОС), необходимо обратиться в техническую поддержку с запросом на добавление нового пакета или обновление версии пакетов РЕД ОС. ■

DNF позволяет взаимодействовать с репозиторием с помощью различных протоколов доступа. Наиболее популярные - HTTP и FTP, однако существуют и некоторые дополнительные методы.

Для того чтобы DNF мог использовать тот или иной репозиторий, информацию о нем необходимо поместить в папку `/etc/yum.repos.d/`

После того как отредактирован список репозиторий в `sources.list`, необходимо обновить локальную базу данных DNF о доступных пакетах. Это делается командой:

```
dnf update
```

При выборе пакетов для установки DNF руководствуется всеми доступными репозиториями вне зависимости от способа доступа к ним. Так, если в репозитории, доступном по сети Интернет, обнаружена более новая версия программы, чем на компакт-диске, то DNF начнёт загружать данный пакет из сети Интернет.

Для создания репозитория, следуйте следующим указаниям:

- Установить пакет `createrepo`:

```
dnf install createrepo
```

- Скопировать все пакеты в один каталог, например:

```
/mnt/local_repo.
```

- Запустить команду «createrepo --database», указав этот каталог:

```
createrepo --database /mnt/local_repo
```

## 5.5 Поиск пакетов

Если пользователь не знает точного названия пакета, для его поиска можно воспользоваться утилитой «dnf search», которая позволяет искать не только по имени пакета, но и по его описанию.

Команда

```
dnf search <подстрока>
```

позволяет найти все пакеты, в именах или описании которых присутствует указанная подстрока.

Для того чтобы подробнее узнать о каждом из найденных пакетов и прочитать его описание, можно воспользоваться командой «dnf info», которая покажет информацию о пакете из репозитория:

```
dnf info gdm-libs
```

## 5.6 Установка или обновление пакета

Установка пакета с помощью DNF выполняется командой:

```
dnf install <имя_пакета>
```

DNF позволяет устанавливать в систему пакеты, требующие для работы другие, пока ещё не установленные. В этом случае он определяет, какие пакеты необходимо установить, и устанавливает их, пользуясь всеми доступными репозиториями.

Команда «dnf install <имя\_пакета>» используется также для обновления уже установленного пакета или группы пакетов. В этом случае dnf дополнительно проверяет, не обновилась ли версия пакета в репозитории по сравнению с установленным в системе.

При помощи DNF можно установить и отдельный бинарный rpm-пакет, не входящий ни в один из репозиториях (например, полученный из Интернет). Для этого достаточно выполнить команду:

```
dnf install <путь_к_файлу.rpm>
```

При этом DNF проведёт стандартную процедуру проверки зависимостей и конфликтов с уже установленными пакетами.

Иногда, в результате операций с пакетами без использования DNF, целостность системы нарушается, и dnf отказывается выполнять операции установки, удаления или обновления. В этом случае необходимо повторить операцию, задав

опцию «-f», заставляющую dnf исправить нарушенные зависимости, удалить или заменить конфликтующие пакеты. В этом случае необходимо внимательно следить за сообщениями, выдаваемыми dnf. Любые действия в этом режиме обязательно требуют подтверждения со стороны пользователя.

## 5.7 Удаление установленного пакета

Для удаления пакета используется команда:

```
dnf remove <имя_пакета>
```

Для того, чтобы не нарушать целостность системы, будут удалены и все пакеты, зависящие от удаляемого: если отсутствует необходимый для работы приложения компонент (например, библиотека), то само приложение становится бесполезным.

## 5.8 Обновление всех установленных пакетов

Чтобы проверить доступные обновления для всех системных пакетов, необходимо выполнить:

```
dnf check-update
```

Когда все пакеты, установленные на сервере, должны быть обновлены, необходимо использовать команду:

```
dnf upgrade
```

## 5.9 Puppet

Puppet - это кроссплатформенная структура, позволяющая системным администраторам выполнять общие задачи с использованием кода. Код позволяет выполнять различные задачи от установки новых программ до проверки прав доступа файлов или обновлений пользовательских учетных записей. В большинстве случаев puppet используется в конфигурации клиент/сервер.

Этот раздел показывает установку и настройку Puppet в конфигурации клиент/сервер. Этот простой пример демонстрирует как установить Apache с использованием Puppet.

Для установки Puppet введите в терминале:

```
dnf install puppet-server
```

На клиентской машине (или машинах) введите:

```
dnf install puppet
```

Прежде чем настраивать puppet, вам, возможно, понадобится добавить запись DNS CNAME для puppet.example.com, где example.com - это ваш домен.

По умолчанию клиенты Puppet проверяют DNS на наличие puppet.example.com в качестве имени puppet сервера (Puppet Master).

Если вы не предполагаете использовать DNS, вы можете добавить записи в файл /etc/hosts на сервере и клиенте. Например, в файл /etc/hosts Puppet-сервера добавьте:

```
127.0.0.1 localhost.localdomain localhost puppet
192.168.1.17 meercat02.example.com meercat02
```

На каждом Puppet клиенте добавьте запись для сервера:

```
192.168.1.16 meercat.example.com meercat puppet
```

**Примечание.** Не забудьте заменить IP-адреса и доменные имена из примера на ваши актуальные адреса и имена сервера и клиентов.

Теперь настроим некоторые ресурсы для Apache HTTP Server. Создайте файл /etc/puppet/code/environments/production/modules/install\_pkg/manifests/init.pp, содержащий следующее:

```
class install_pkg {
  package {
    'Apache HTTP Server':
    ensure => installed
  }
  service {
    'Apache HTTP Server':
    ensure => true,
    enable => true,
    require => Package['Apache HTTP Server']
  }
}
```

Обратите внимание, что был создан класс «install\_pkg», совпадающий с именем модуля «install\_pkg». Модули — это возможность использовать классы и функции в puppet. Модуль — это всего лишь директория с предопределённой структурой каталогов и файлов. Выглядит структура модуля примерно так: <имя\_модуля>/

- files/ - содержит различные файлы;
- lib/ - содержит плагины, например, особые переменные (facts) или типы ресурсов (может вы создадите свой file\_yours тип);
- manifests/ - хранит все манифесты;
- init.pp - должен быть обязательно;
- <класс1>.pp;
- <определяемый\_тип>.pp;
- <класс1>/;
- <под\_класс1>.pp;
- <под\_класс2>.pp;

- `templates/` - содержит используемые шаблоны «\*.erb»;
  - `tests/`;
- Обращение в коде puppet к классам будет выглядеть как:

```
<имя_модуля> { ... }  
<имя_модуля>::<класс1> { ... }  
<имя_модуля>::<класс1>::<под_класс1> { ... }
```

Для того, чтобы модуль вообще заработал достаточно иметь папку с именем модуля, папку с манифестами и начальным манифестом «init.pp».

Требуется, чтобы в каждом из файлов `<класс1> ... <под_класс1>` был один и только один класс с соответствующим именем: `<имя_модуля>::<класс1> ... <имя_модуля>::<класс1>::<под_класс1>`. При этом файл `init.pp` должен содержать класс с именем `<имя_модуля>`.

Получить доступ к файлам модуля можно, например, по адресу `puppet:///modules/<имя_модуля>/`.

Далее создайте файл узла `/etc/puppet/code/environments/production/manifests/site.pp` со следующим содержимым:

```
node 'meercat02.example.com' {  
  include install_pkg  
}
```

Замените «meercat02.example.com» на актуальное имя вашего Puppet клиента. Используйте для имени ноды ключевое слово `default`, если необходимо применить настройки для всех узлов.

Финальным шагом для этого простого Puppet сервера является перезапуск сервиса:

```
systemctl restart /etc/init.d/puppetmaster
```

Теперь на Puppet сервере все настроено и время настроить клиента.

Сначала настроим сервис Puppet агента для запуска.

Отредактируйте `/etc/default/puppet`, заменив значение «START» на «yes»:

```
START=yes
```

Далее запустите сервис:

```
systemctl start /etc/init.d/puppet
```

Возвращаемся на Puppet сервер для подписи клиентского сертификата с помощью команды:

```
puppetca --sign meercat02.example.com
```

Проверьте `/var/log/syslog` на любые ошибки конфигурации. Если все прошло хорошо, пакет Apache HTTP Server и его зависимости будут установлены на

Руррет клиенте.

# Система безопасности РЕД ОС

## 6. Система безопасности РЕД ОС

### 6.1 Программа sudo

sudo - это программа, разработанная в помощь системному администратору и позволяющая делегировать те или иные привилегированные ресурсы пользователям с ведением протокола работы. Основная идея - дать пользователям как можно меньше прав, но при этом ровно столько, сколько необходимо для решения поставленных задач.

Команда sudo предоставляет возможность пользователям выполнять команды от имени root либо других пользователей. Правила, используемые sudo для принятия решения о предоставлении доступа, находятся в файле /etc/sudoers. Кроме того, пример правил, предоставляющих пользователям, являющимся членами группы grp, возможность устанавливать, обновлять и удалять пакеты в системе, приведён в файле /usr/share/doc/sudo-<версия>/sample.sudoers.

Для редактирования файла /etc/sudoers следует использовать программу visudo, которая проверяет синтаксис и тем самым позволяет избежать ошибок в правилах.

В большинстве случаев грамотная настройка sudo делает работу от имени суперпользователя ненужной.

### 6.2 IP-фильтр iptables: архитектура и синтаксис

Назначение IP-фильтра - обработка потока данных, проходящих через стек сетевых протоколов ядра ОС по заданным критериям.

Фильтры состоят из правил. Каждое правило - это строка, содержащая в себе критерии, определяющие, подпадает ли пакет под заданное правило, и действие, которое необходимо выполнить в случае удовлетворения критерия.

### 6.2.1 Устройство фильтра iptables

Для iptables в общем виде правила выглядят так:

```
iptables <-t table> command <match> <target/jump>
```

Не обязательно ставить описание действия <target/jump> последним в строке, но лучше придерживаться именно такой нотации для удобочитаемости правил.

Если в правило не включается спецификатор <-t table>, то по умолчанию предполагается использование таблицы «filter», если же предполагается использование другой таблицы, то это требуется указать явно. Спецификатор таблицы так же можно указывать в любом месте строки правила, однако более или менее стандартом считается указание таблицы в начале правила.

Далее, непосредственно за именем таблицы должна стоять команда управления фильтром. Если спецификатора таблицы нет, то команда всегда должна стоять первой. Команда определяет действие iptables, например: вставить правило, или добавить правило в конец цепочки, или удалить правило и т.п. Тело команды в общем виде выглядит так:

```
<команда> <цепочка>
```

Ключ команды указывает на то, что нужно сделать с правилом, например, команда «-A» указывает на то, что правило нужно добавить в конец указанной цепочки.

Цепочка указывает в какую цепочку нужно добавить правило. Стандартные цепочки - INPUT, OUTPUT, FORWARD, PREROUTING и POSTROUTING. Они находятся в таблицах фильтра. Не все таблицы содержат все стандартные цепочки.

Раздел <match> задаёт критерии проверки, по которым определяется, подпадает ли пакет под действие этого правила или нет. Здесь можно указать самые разные критерии - IP-адрес источника пакета или сети, сетевой интерфейс и т.д.

<target> указывает, какое действие должно быть выполнено при условии выполнения критериев в правиле. Здесь можно передать пакет в другую цепочку правил, «сбросить» пакет и забыть про него, выдать на источник сообщение об ошибке и т.д.

Когда пакет приходит на сетевое устройство, он обрабатывается соответствующим драйвером и далее передается в фильтр в ядре ОС. Далее пакет проходит ряд таблиц и затем передаётся либо локальному приложению, либо переправляется на другую машину.

### 6.2.2 Встроенные таблицы фильтра iptables

По умолчанию используется таблица «filter». Опция «-t» в правиле указывает на используемую таблицу. С ключом «-t» можно указывать следующие таблицы: «nat», «mangle», «filter».

### Таблица nat

Таблица «nat» используется, главным образом, для преобразования сетевых адресов Network Address Translation. Через эту таблицу проходит только первый пакет из потока. Преобразования адресов автоматически применяется ко всем последующим пакетам. Это один из факторов, исходя из которых, не нужно осуществлять какую-либо фильтрацию в этой таблице.

Цепочка PREROUTING используется для внесения изменений в пакеты на входе в фильтр.

Цепочка OUTPUT используется для преобразования пакетов, созданных приложениями внутри компьютера, на котором установлен фильтр, перед принятием решения о маршрутизации.

Цепочка POSTROUTING используется для преобразования пакетов перед выдачей их в сеть.

### Таблица mangle

Таблица «mangle» используется для внесения изменений в заголовки пакетов. Примером может служить изменение поля TTL, TOS или MARK.

**Важно!** В действительности поле MARK не изменяется, но в памяти ядра заводится структура, которая сопровождает данный пакет все время его прохождения через машину так, что другие правила и приложения на данной машине (и только на данной машине) могут использовать это поле в своих целях. Таблица имеет две цепочки PREROUTING и OUTPUT. ■

Цепочка PREROUTING используется для внесения изменений на входе в фильтр перед принятием решения о маршрутизации.

Цепочка OUTPUT – для внесения изменений в пакеты, поступающие от внутренних приложений. Таблица «mangle» не должна использоваться для преобразования сетевых адресов (Network Address Translation) или маскардинга (masquerading), поскольку для этих целей имеется таблица «nat».

### Таблица filter

Таблица filter используется главным образом для фильтрации пакетов. Для примера, здесь мы можем выполнить DROP, LOG, ACCEPT или REJECT без каких-либо сложностей, как в других таблицах. Имеется три встроенных цепочки FORWARD, INPUT, OUTPUT.

Цепочка FORWARD используется для фильтрации пакетов, идущих транзитом через фильтрующий компьютер.

Цепочка INPUT предназначена для обработки входящих пакетов, направляемых локальным приложениям фильтрующего компьютера.

Цепочка OUTPUT используется для фильтрации исходящих пакетов, сгенерированных локальными приложениями фильтрующего компьютера.

## 6.2.3 Команды утилиты iptables

Ниже приводится список команд и правила их использования. Посредством команд сообщается iptables, что предполагается сделать. Обычно предполагается одно из двух действий - это добавление нового правила в цепочку или удаление

существующего правила из той или иной таблицы. Далее приведены команды, которые используются в iptables.

Команда	Формат вызова	Результат
-A, -append	iptables -A INPUT	Добавляет новое правило в конец заданной цепочки.
-D, -delete	iptables -D INPUT, -dport 80 -j DROP, iptables -D INPUT 1	Удаление правила из цепочки. Команда имеет два формата записи, первый - когда задаётся критерий сравнения с опцией -D (см. первый пример), второй - порядковый номер правила. Если задаётся критерий сравнения, то удаляется правило, которое имеет в себе этот критерий, если задаётся номер правила, то будет удалено правило с заданным номером. Счёт правил в цепочках начинается с 1.
-R, -replace	iptables -R INPUT 1 -s 192.168.0.1 -j DROP	Данная команда заменяет одно правило другим. В основном она используется во время отладки новых правил.
-I, -insert	iptables -I INPUT 1 -dport 80 -j АСЦЕПТ	Вставляет новое правило в цепочку. Число, следующее за именем цепочки, указывает номер правила, перед которым нужно вставить новое правило, другими словами число задаёт номер для вставляемого правила. В примере, указывается, что данное правило должно быть 1-м в цепочке INPUT.
-L, -list	iptables -L INPUT	Вывод списка правил в заданной цепочке, в данном примере предполагается вывод правил из цепочки INPUT. Если имя цепочки не указывается, то выводится список правил для всех цепочек. Формат вывода зависит от наличия дополнительных ключей в команде, например -n, -v, и пр.
-F, -flush	iptables -F INPUT	Удаление всех правил из заданной цепочки (таблицы). Если имя цепочки и таблицы не указывается, то удаляются все правила, во всех цепочках.

Команда	Формат вызова	Результат
<code>-Z, -zero</code>	<code>iptables -Z INPUT</code>	Обнуление всех счётчиков в заданной цепочке. Если имя цепочки не указывается, то подразумеваются все цепочки. При использовании ключа <code>-v</code> совместно с командой <code>-L</code> , на вывод будут поданы и состояния счётчиков пакетов, попавших под действие каждого правила. Допускается совместное использование команд <code>-L</code> и <code>-Z</code> . В этом случае будет выдан сначала список правил со счётчиками, а затем произойдёт обнуление счётчиков.
<code>-N, -new-chain</code>	<code>iptables -N allowed</code>	Создаётся новая цепочка с заданным именем в заданной таблице <code>B</code> выше приведённом примере создаётся новая цепочка с именем <code>allowed</code> . Имя цепочки должно быть уникальным и не должно совпадать с зарезервированными именами цепочек и действий ( <code>DROP</code> , <code>REJECT</code> и т.п.)
<code>-X, -delete -chain</code>	<code>iptables -X allowed</code>	Удаление заданной цепочки из заданной таблицы. Удаляемая цепочка не должна иметь правил и не должно быть ссылок из других цепочек на удаляемую цепочку. Если имя цепочки не указано, то будут удалены все цепочки, определённые командой <code>-N</code> в заданной таблице.
<code>-P, -policy</code>	<code>iptables -P INPUT DROP</code>	Определяет политику по умолчанию для заданной цепочки. Политика по умолчанию определяет действие, применяемое к пакетам не попавшим под действие ни одного из правил в цепочке. В качестве политики по умолчанию допускается использовать <code>DROP</code> , <code>ACCEPT</code> и <code>REJECT</code> .
<code>-E, -rename -chain</code>	<code>iptables -E allowed disallowed</code>	Команда <code>-E</code> выполняет переименование пользовательской цепочки. В примере цепочка <code>allowed</code> будет переименована в цепочку <code>disallowed</code> . Эти переименования не изменяют порядок работы, а носят только косметический характер.

Команда должна быть указана всегда. Список доступных команд можно просмотреть с помощью команды:

```
iptables -h
```

или, что то же самое:

```
iptables -help
```

Некоторые команды могут использоваться совместно с дополнительными ключами. Ниже приводится список дополнительных ключей, и описывается результат их действия.

#### 6.2.4 Ключи утилиты iptables

Ключ	Пример	Пояснения
-v, -verbose	-list, -append, -insert, -delete, -replace	Данный ключ используется для повышения информативности вывода и, как правило, используется совместно с командой -list. В случае использования с командой -list, в вывод этой команды включаются так же имя интерфейса, счётчики пакетов и байт для каждого правила. Формат вывода счётчиков предполагает вывод кроме цифр числа ещё и символьные множители К (x1000), М (x1,000,000) и G (x1,000,000,000). Для того чтобы заставить команду -list выводить полное число (без употребления множителей), требуется применять ключ -x, который описан ниже. Если ключ -v, -verbose используется с командами -append, -insert, -delete или -replace, то на вывод будет выдан подробный отчёт о произведённой операции.
-x, -exact	-list	Для всех чисел в выходных данных выводятся их точные значения без округления и без применения множителей К, М, G.
-n, -numeric	-list	Iptables выводит IP-адреса и номера портов в числовом виде, предотвращая попытки преобразовать их в символические имена.
-line-number	-list	Ключ -line-numbers включает режим вывода номеров строк при отображении списка правил.
-c, -set -counters	-insert, -append, -replace	Этот ключ используется при создании нового правила для установки счётчиков пакетов и байт в заданное значение. Например, ключ -set-counters 20 4000 установит счётчик пакетов = 20, а счётчик байт = 4000.
-modprobe	Любая команда	Ключ -modprobe определяет команду загрузки модуля ядра.

#### 6.2.5 Основные действия над пакетами в фильтре iptables

Действие	Пояснения
ACCEPT	Пакет прекращает движение по цепочке (и всем вызвавшим цепочкам, если текущая цепочка была вложенной) и считается принятым; тем не менее, пакет продолжит движение по цепочкам в других таблицах и может быть отвергнут там.
DROP	Отбрасывает пакет и iptables «забывает» о его существовании. Отброшенные пакеты прекращают своё движение полностью.
RETURN	Прекращает движение пакета по текущей цепочке правил и производит возврат в вызывающую цепочку, если текущая цепочка была вложенной, или, если текущая цепочка лежит на самом верхнем уровне (например INPUT), то к пакету будет применена политика по умолчанию.
LOG	Служит для журналирования отдельных пакетов и событий. В системный журнал могут заноситься заголовки IP-пакетов и другая интересующая вас информация.
REJECT	Используется, как правило, в тех же самых ситуациях, что и DROP, но в отличие от DROP, команда REJECT выдаёт сообщение об ошибке на хост, передавший пакет.
SNAT	Используется для преобразования сетевых адресов (Source Network Address Translation), т.е. изменение исходящего IP-адреса в IP-заголовке пакета.
DNAT	Destination Network Address Translation используется для преобразования адреса места назначения в IP-заголовке пакета.
MASQUERADE	В основе своей представляет то же самое, что и SNAT только не имеет ключа -to -source. Причиной служит то, что маскарадинг может работать, например, с dialup подключением или DHCP, т.е. в тех случаях, когда IP-адрес присваивается устройству динамически. Если используется динамическое подключение, то нужно использовать маскарадинг, если же используется статическое IP-подключение, то лучшим выходом будет использование действия SNAT.
REDIRECT	Выполняет перенаправление пакетов и потоков на другой порт той же самой машины. К примеру, можно пакеты, поступающие на HTTP порт перенаправить на порт HTTP proxy. Действие REDIRECT очень удобно для выполнения «прозрачного» проксирования (transparent proxy), когда компьютеры в локальной сети даже не подозревают о существовании прокси.

Действие	Пояснения
TTL	Используется для изменения содержимого поля «время жизни» (Time To Live) в IP-заголовке. Один из вариантов применения этого действия - это устанавливать значение поля Time To Live во всех исходящих пакетах в одно и то же значение. Если установить на все пакеты одно и то же значение TTL, то тем самым можно лишить провайдера одного из критериев определения того, что подключение к Интернету разделяется между несколькими компьютерами. Для примера можно привести число TTL = 64, которое является стандартным для ядра ОС.

### 6.2.6 Основные критерии пакетов в фильтре iptables

Критерий	Пояснения
-p, -protocol	Используется для указания типа протокола. Примерами протоколов могут быть TCP, UDP и ICMP. Список протоколов можно посмотреть в файле /etc/protocols. Прежде всего, в качестве имени протокола в данный критерий можно передавать три вышеупомянутых протокола, а также ключевое слово ALL. В качестве протокола допускается передавать число - номер протокола
-s, -src, -source	IP-адрес (-a) источника пакета. Адрес источника может указываться так - 192.168.1.1, тогда подразумевается единственный IP-адрес. А можно указать адрес в виде address/mask, например как 192.168.0.0/255.255.255.0, или более современным способом 192.168.0.0/24, т.е. фактически определяя диапазон адресов. Символ «!», установленный перед адресом, означает логическое отрицание, т.е. -source ! 192.168.0.0/24 означает любой адрес, кроме адресов 192.168.0.x.
-d, -dst, -destination	IP-адрес (-a) получателя. Имеет синтаксис, схожий с критерием -source, за исключением того, что подразумевает адрес места назначения. Точно так же может определять как единственный IP-адрес, так и диапазон адресов. Символ «!» используется для логической инверсии критерия.
-i, -in -interface	Интерфейс, с которого был получен пакет. Использование этого критерия допускается только в цепочках INPUT, FORWARD и PREROUTING, в любых других случаях будет вызывать сообщение об ошибке.
-o, -out -interface	Задаёт имя выходного интерфейса. Этот критерий допускается использовать только в цепочках OUTPUT, FORWARD и POSTROUTING, в противном случае будет генерироваться сообщение об ошибке.

Критерий	Пояснения
-f, -fragment	Правило распространяется на все фрагменты фрагментированного пакета, кроме первого, сделано это потому, что нет возможности определить исходящий/входящий порт для фрагмента пакета, а для ICMP-пакетов определить их тип. С помощью фрагментированных пакетов могут производиться атаки на межсетевой экран, так как фрагменты пакетов могут не отлавливаться другими правилами.
-sport, -source-port	Исходный порт, с которого был отправлен пакет. В качестве параметра может указываться номер порта или название сетевой службы. Соответствие имён сервисов и номеров портов вы сможете найти в файле /etc/services. При указании номеров портов правила обрабатываются несколько быстрее.
-dport, -destination -port	Порт, на который адресован пакет. Аргументы задаются в том же формате, что и для -source-port.
-tcp-flags	SYN,ACK,FIN SYN Определяет маску и флаги tcp-пакета. Пакет считается удовлетворяющим критерию, если из перечисленных флагов в первом списке в единичное состояние установлены флаги из второго списка. В качестве аргументов критерия могут выступать флаги SYN, ACK, FIN, RST, URG, PSH, а так же зарезервированные идентификаторы ALL и NONE. ALL - значит ВСЕ флаги и NONE - НИ ОДИН флаг. Так, критерий -tcp-flags ALL NONE означает, что все флаги в пакете должны быть сброшены. Как и ранее, символ «!» означает инверсию критерия. Имена флагов в каждом списке должны разделяться запятыми, пробелы служат для разделения списков.
-icmp-type	Тип сообщения ICMP определяется номером или именем. Числовые значения определяются в RFC 792. Чтобы получить список имен ICMP значений выполните команду iptables -protocol icmp ^^. Символ «!» инвертирует критерий, например -icmp-type ! 8.

Критерий	Пояснения
-state	<p>Для использования данного критерия в правиле перед -state нужно явно указать -m state. Проверяется признак состояния соединения. Можно указывать 4 состояния: INVALID, ESTABLISHED, NEW и RELATED.</p> <p>INVALID подразумевает, что пакет связан с неизвестным потоком или соединением и, возможно содержит ошибку в данных или в заголовке.</p> <p>ESTABLISHED указывает на то, что пакет принадлежит уже установленному соединению, через которое пакеты идут в обоих направлениях.</p> <p>NEW подразумевает, что пакет открывает новое соединение или пакет принадлежит однонаправленному потоку.</p> <p>RELATED указывает на то, что пакет принадлежит уже существующему соединению, но при этом он открывает новое соединение. Примером тому может служить передача данных по FTP, или выдача сообщения ICMP об ошибке, которое связано с существующим TCP или UDP соединением.</p> <p>Признак NEW - это не то же самое, что установленный бит SYN в пакетах TCP, посредством которых открывается новое соединение, и, подобного рода пакеты могут быть потенциально опасны в случае, когда для защиты сети используется один сетевой экран.</p>

### 6.2.7 Использование фильтра iptables

РЕД ОС уже включает в себя предустановленный iptables. Для его настройки рекомендуется использовать возможности системы настройки сети /etc/netconfig и /etc/networks.

## 6.3 Аудит в РЕД ОС

### 6.3.1 Файлы и утилиты аудита РЕД ОС

Набор утилит управления РЕД ОС находится в главном меню - «Центр управления». Большинство утилит управления и конфигурирования РЕД ОС требуют привилегий администратора РЕД ОС.

#### Описание auditd.conf

В файле /etc/audit/auditd.conf определяются параметры службы аудита. На одной строке может быть не больше одной директивы. Директива состоит из ключевого слова (названия параметра), знака равенства и соответствующих ему данных (значения параметра). Допустимые ключевые слова приведены в таблице.

Ключ	Значение ключа
<code>&lt;log_file&gt;</code>	Полное имя файла, в который следует записывать протокол.
<code>&lt;log_format&gt;</code>	Оформление данных в протоколе. Допустимы два значения: raw и nolog. При указании RAW, данные будут записываться в том виде, в котором они получаются от ядра. Значение NOLOG отключает запись данных об аудите. Этот параметр не влияет на обработку данных диспетчером событий системы аудита.
<code>&lt;priority_boost&gt;</code>	Неотрицательное число, определяющее повышение приоритета выполнения службы аудита. Значение по умолчанию: 3. Для того чтобы не изменять приоритет, укажите 0.
<code>&lt;flush&gt;</code>	Стратегия работы с дисковым буфером. Допустимые значения: none, incremental, data и sync. Вариант none, отключает какие-либо дополнительные действия со стороны службы по синхронизации буфера с диском. При значении incremental запросы на перенос данных из буфера на диск выполняются с частотой, задаваемой параметром freq. При значении data данные файла синхронизируются немедленно. Значение sync указывает на необходимость немедленной синхронизации как данных, так и метаданных файла при записи на диск.
<code>&lt;freq&gt;</code>	Максимальное число записей протокола, которые могут храниться в буфере. При достижении этого числа производится запись буферизованных данных на диск. Данный параметр допустим, только если flush имеет значение incremental.
<code>&lt;num_logs&gt;</code>	Максимальное число файлов с протоколами. Используется, если параметр <code>&lt;max_log_file_action&gt;</code> имеет значение rotate. Если указано число меньше 2, при достижении ограничения на размер файла он обнуляется. Значение параметра не должно превышать 99. Значение по умолчанию: 0. При указании большого числа может потребоваться увеличить ограничение на количество ожидающих запросов. Это можно сделать в файле <code>/etc/audit/audit.rules</code> .
<code>&lt;dispatcher&gt;</code>	Диспетчер - программа, которой (на стандартный ввод) будут передаваться копии сообщений о событиях аудита. Она запускается (с правами администратора) службой аудита при загрузке последней.

Ключ	Значение ключа
<disp_qos>	Разрешить ли блокирование при взаимодействии с диспетчером. Для передачи информации диспетчеру используется буфер размером 128 кб. Это значение является оптимальным для большинства случаев. Если блокирование запрещено (lossy), то все сообщения, поступающие при полном буфере, не будут доходить до диспетчера (записи о них по-прежнему будут вноситься в файл на диске, если только <log_format> не равно nolog). В случае, если блокирование разрешено (lossless), служба аудита будет ожидать появления свободного места в очереди, передавать сообщение диспетчеру и только потом записывать его на диск. Допустимые значения: lossy и lossless. Значение по умолчанию - lossy.
<max_log_file>	Ограничение на размер файла протокола в мегабайтах. Действие, выполняемое при достижении размера файла указанного значения, можно настроить с помощью следующего параметра.
<max_log_file_action>	Действие, предпринимаемое при достижении размером файла протокола максимального значения. Допустимые значения: ignore, syslog, suspend, rotate и keep_logs. Вариант ignore, отключает контроль над размером файла. При значении syslog в системный протокол будет внесено соответствующее сообщение. При значении suspend дальнейшее ведение протокола будет прекращено. Служба по-прежнему будет работать. При значении rotate текущий файл будет переименован и для протокола будет создан новый файл. Имя предыдущего протокола будет дополнено числом 1, а номера других протоколов (если они имеются) будут увеличены на единицу. Таким образом, чем больше номер у протокола, тем он старше. Максимальное число файлов определяется параметром <num_logs> (естественно, соответствие ему достигается за счёт удаления самых старых протоколов). Такое поведение аналогично поведению утилиты logrotate. Вариант keep_logs аналогичен предыдущему, но число файлов не ограничено.
<action_mail_acct>	Адрес электронной почты. Значение по умолчанию: root. Если адрес не локальный по отношению к данной системе, необходимо чтобы в ней был настроен механизм отправки почты. В частности, требуется наличие программы /usr/lib/sendmail.
<space_left>	Минимум свободного пространства в мегабайтах, при достижении которого должно выполняться действие, определяемое следующим параметром.

Ключ	Значение ключа
<space_left_action>	<p>Действие, предпринимаемое при достижении объёмом свободного пространства на диске указанного минимума. Допустимые значения - ignore, syslog, email, exes, suspend, single и halt. При значении ignore, никаких действий не производится. При значении syslog в системный протокол добавляется соответствующая запись. При значении email по адресу, указанному в &lt;action_mail_acct&gt;, отправляется уведомление. При значении exes &lt;путь_к_программе&gt; запускается программа по указанному пути. Передача параметров не поддерживается. При значении suspend служба аудита прекратит вести протокол событий на диске, но будет продолжать работать. Указание single приведёт к переводу компьютера в однопользовательский режим. Указание halt приведёт к выключению компьютера.</p>
<admin_space_left>	<p>Критический минимум свободного пространства в мегабайтах, при достижении которого должно выполняться действие, определяемое следующим параметром. Данное действие следует рассматривать как последнюю меру, предпринимаемую перед тем, как закончится место на диске. Значение настоящего параметра должно быть меньше значения &lt;space_left&gt;.</p>
<admin_space_left_action>	<p>Действие, предпринимаемое при достижении объёмом свободного пространства на диске указанного критического минимума. Допустимые значения - ignore, syslog, email, exes, suspend, single и halt. При значении ignore, никаких действий не производится. При значении syslog в системный протокол добавляется соответствующая запись. При значении email по адресу, указанному в &lt;action_mail_acct&gt;, отправляется уведомление. При значении exes &lt;путь_к_программе&gt; запускается программа по указанному пути. Передача параметров не поддерживается. При значении suspend служба аудита прекратит вести протокол событий на диске, но будет продолжать работать. Указание single приведёт к переводу компьютера в однопользовательский режим. Указание halt приведёт к выключению компьютера.</p>

Ключ	Значение ключа
<code>&lt;disk_full_action&gt;</code>	<p>Действие, предпринимаемое при обнаружении отсутствия свободного пространства на диске. Допустимые значения - ignore, syslog, email, exes, suspend, single и halt. При значении ignore, никаких действий не производится. При значении syslog в системный протокол добавляется соответствующая запись. При значении email по адресу, указанному в <code>&lt;action_mail_acct&gt;</code>, отправляется уведомление. При значении exes <code>&lt;/некоторый_путь&gt;</code> запускается сценарий по указанному пути. Передача параметров сценарию не поддерживается. При значении suspend служба аудита прекратит вести протокол событий на диске, но будет продолжать работать. Указание single приведёт к переводу компьютера в однопользовательский режим. Указание halt приведёт к выключению компьютера.</p>
<code>&lt;disk_error_action&gt;</code>	<p>Действие, предпринимаемое при возникновении ошибки в работе с диском. Допустимые значения - ignore, syslog, email, exes, suspend, single и halt. При значении ignore, никаких действий не производится. При значении syslog в системный протокол добавляется соответствующая запись. При значении email по адресу, указанному в <code>&lt;action_mail_acct&gt;</code>, отправляется уведомление. При значении exes <code>&lt;/некоторый_путь&gt;</code> запускается сценарий по указанному пути. Передача параметров сценарию не поддерживается. При значении suspend служба аудита прекратит вести протокол событий на диске, но будет продолжать работать. Указание single приведёт к переводу компьютера в однопользовательский режим. Указание halt приведёт к выключению компьютера.</p>

Для обеспечения полного использования раздела параметрам `<max_log_file>` и `<num_logs>` следует присвоить соответствующие значения. Учитывайте, что чем больше файлов создаётся на диске (и соответственно переименовывается), тем больше времени будет уходить на обработку событий при достижении размером очередного файла максимума. Параметру `<max_log_file_action>` рекомендуется присвоить значение `keep_logs`.

Значение `<space_left>` должно быть таким, которое позволит администратору вовремя среагировать на предупреждение. Обычно в число действий выполняемых администратором входит запуск `auditport -t` и архивирование самых старых протоколов. Значение `<space_left>` зависит от системы, в частности от частоты поступления сообщений о событиях. Значение `<space_left_action>` рекомендуется установить в `email`. Если требуется отправка сообщения `snmp trap`, укажите вариант `exes`.

Установите значение `<admin_space_left>` таким образом, чтобы хватило

свободного места для сохранения записей о последующих действиях администратора. Значение параметра `<admin_space_left_action>` следует установить в `single`, ограничив, таким образом, способы взаимодействия с системой консолью.

Действие, указанное в `<disk_full_action>`, выполняется, когда в разделе уже не осталось свободного места. Доступ к ресурсам машины должен быть полностью прекращён, т.к. нет возможности контролировать работу системы. Это можно сделать, указав значение `single` или `halt`.

Значение `<disk_error_action>` следует установить в `syslog`, `single`, либо `halt` в зависимости от соглашения относительно обращения со сбойным аппаратным обеспечением.

### Служба аудита - auditd

Служба `auditd` – это прикладной компонент системы аудита. Он ведёт протокол аудита на диске. Для просмотра протоколов предназначены команды `auresearch` и `aureport`. Команда `auditctl` позволяет настраивать правила аудита. Кроме того, при загрузке загружаются правила из файла `/etc/audit/auditd.rules`. Некоторые параметры самой службы можно изменить в файле `auditd.conf`.

Синтаксис:

```
auditd <-f> <-l> <-n>
```

Основные опции службы `auditd` приведены в таблице.

Опция	Описание опции
<code>-f</code>	не переходить в фоновый режим (для отладки). Сообщения программы будут направляться в стандартный вывод для ошибок ( <code>stderr</code> ), а не в файл.
<code>-l</code>	включить следование по символическим ссылкам при поиске конфигурационных файлов.
<code>-n</code>	не создавать дочерний процесс. Для запуска из <code>inittab</code> .

Основные сигналы, используемые службой `auditd`, описаны в таблице.

Сигнал	Описание сигнала
<code>SIGHUP</code>	Перезагрузить конфигурацию - загрузить файл конфигурации с диска. Если в файле не окажется синтаксических ошибок, внесенные в него изменения вступят в силу. При этом в протокол будет добавлена запись о событии <code>DAEMON_CONFIG</code> . В противном случае действия службы будут зависеть от параметров <code>&lt;space_left_action&gt;</code> , <code>&lt;admin_space_left_action&gt;</code> , <code>&lt;disk_full_action&gt;</code> , <code>&lt;disk_error_action&gt;</code> файла <code>auditd.conf</code> .
<code>SIGTERM</code>	прекратить обработку событий аудита и завершить работу, о чём предварительно занести запись в протокол.

Сигнал	Описание сигнала
SIGUSR1	создать новый файл для протокола, перенумеровав старые файлы или удалив часть из них, в зависимости от параметра <code>&lt;max_log_size_action&gt;</code> .

**Важно!** Для того чтобы сделать возможным аудит всех процессов, запущенных до службы аудита, добавьте в строку параметров ядра (в конфигурации загрузчика) `audit=1`. В противном случае аудит некоторых процессов будет невозможен. ■

### Утилита `auditctl`

Утилита `auditctl` используется для контроля поведения, получения состояния и добавления/удаления правил аудита, предоставляемого ядром.

Основные опции утилиты `auditctl` приведены в таблице.

Опция	Значение опции
<code>-b backlog</code>	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.
<code>-e [0..2]</code>	Установить флаг блокировки. «0» позволит на время отключить аудит, включить его обратно можно, передав «1» как параметр. Если установлено значение опции «2», то защитит конфигурацию аудита от изменений. Каждый, кто захочет воспользоваться этой возможностью, может поставить эту команду последней в <code>audit.rules</code> . 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.
<code>-f [0..2]</code>	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 службы 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 предпочтительно.
<code>-h</code>	Краткая помощь по аргументам командной строки.
<code>-i</code>	Игнорировать ошибки при чтении правил из файла.
<code>-l</code>	Вывести список всех правил по одному правилу в строке.

Опция	Значение опции
-k <ключ>	Установить на правило ключ фильтрации. Ключ фильтрации - это произвольная текстовая строка длиной не больше 31 символа. Ключ помогает уникально идентифицировать записи, генерируемые в ходе аудита за точкой наблюдения.
-m <текст>	Послать в систему аудита пользовательское сообщение. Это может быть сделано только из-под учётной записи root.
-p [r w x a]	Установить фильтр прав доступа для точки наблюдения. r=чтение, w=запись, x=исполнение, a=изменение атрибута. Не путайте эти права доступа с обычными правами доступа к файлу - они определяют типы системных вызовов, которые выполняют данные действия. Заметьте, системные вызовы read и write не включены в этот набор, поскольку логи аудита были бы перегружены информацией о работе этих вызовов.
-r <частота>	Установить ограничение скорости выдачи сообщений в секунду (0 - нет ограничения). Если эта частота не нулевая и она превышает в ходе аудита, флаг сбоя выставляется ядром для выполнения соответствующего действия. Значение по умолчанию: 0.
-R <файл>	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. Файл может содержать комментарии, начинающиеся с символа «#». Правила, расположенные в файле, идентичны тем, что набираются в командной строке, без указания «auditctl».
-s	Получить статус аудита.
-a <список>, <действие>	Добавить правило с указанным действием к концу списка. Заметьте, что запятая разделяет эти два значения. Отсутствие запятой вызовет ошибку. Ниже описаны имена доступных списков.
task	Добавить правило к списку, отвечающему за процессы. Этот список правил используется только во время создания процесса - когда родительский процесс вызывает fork() или clone(). При использовании этого списка вы можете использовать только те поля, которые известны во время создания процесса: uid, gid и т.д.
entry	Добавить правило к списку, отвечающему за точки входа системных вызовов. Этот список применяется, когда необходимо создать событие для аудита, привязанное к точкам входа системных вызовов.

Опция	Значение опции
<code>exit</code>	Добавить правило к списку, отвечающему за точки выхода из системных вызовов. Этот список применяется, когда необходимо создать событие для аудита, привязанное к точкам выхода из системных вызовов.
<code>user</code>	Добавить правило, отвечающее за список фильтрации пользовательских сообщений. Этот список используется ядром, чтобы отфильтровать события, приходящие из пользовательского пространства, перед тем как они будут переданы службе аудита. Необходимо отметить, что только следующие поля могут быть использованы: <code>uid</code> , <code>auid</code> , <code>gid</code> и <code>pid</code> . Все остальные поля будут обработаны, как если бы они не совпали.
<code>exclude</code>	Добавить правило к списку, отвечающему за фильтрацию событий определённого типа. Этот список используется, чтобы отфильтровывать ненужные события. Например, если вы не хотите видеть <code>avc</code> сообщения, вы должны использовать этот список. Тип сообщения задаётся в поле <code>msgtype</code> .

В нижеприведенной таблице описаны доступные действия для правил:

Действие	Описание действия
<code>never</code>	Аудит не будет генерировать никаких записей. Это может быть использовано для подавления генерации событий. Обычно необходимо подавлять генерацию сверху списка, а не внизу, т.к. событие инициируется на первом совпавшем правиле.
<code>always</code>	Установить контекст аудита. Всегда заполнять его во время входа в системный вызов и всегда генерировать запись во время выхода из системного вызова.
<code>-A &lt;список&gt;, &lt;действие&gt;</code>	Добавить правило с указанным действием в начало списка.
<code>-d &lt;список&gt;, &lt;действие&gt;</code>	Удалить правило с указанным действием из списка. Правило удаляется только в том случае, если полностью совпали и имя системного вызова и поля сравнения.
<code>-D</code>	Удалить все правила и точки наблюдения.
<code>-S &lt;имя или номер системного вызова&gt;</code>	Любой номер или имя системного вызова может быть использован. Также возможно использование ключевого слова <code>all</code> . 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.

Действие	Описание действия
-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. Вы можете задать до 64 полей сравнения в одной команде. Каждое новое поле должно начинаться с -F. Аудит будет генерировать запись, если произошло совпадение по всем полями сравнения. Допустимо использование одного из следующих 8 операторов: равно, не равно, меньше, больше, меньше либо равно, больше либо равно, битовая маска (n&v) и битовая проверка (n&=v). Битовая проверка выполняет операцию «and» над значениями и проверяет, равны ли они. Битовая маска просто выполняет операцию «and». Поля, оперирующие с идентификатором пользователя, могут также работать с именем пользователя - программа автоматически получит идентификатор пользователя из его имени. То же самое можно сказать и про имя группы.

Поля сравнения могут быть заданы для следующих объектов: четыре первых аргумента, переданных системному вызову. Строковые аргументы не поддерживаются. Это связано с тем, что ядро должно получать указатель на строку, а проверка поля по значению адреса указателя не желательна. Таким образом, необходимо использовать только цифровые значения.

Поле сравнения	Описание
arch	Архитектура процессора, на котором выполняется системный вызов. Используйте «uname -m», чтобы определить архитектуру. Если вы не знаете архитектуру вашей машины, но хотите использовать таблицу 32-х битных системных вызовов, и ваша машина поддерживает 32 бита, вы можете использовать x32. Подобно этому x64 может быть использовано для использования таблицы 64-х битных системных вызовов.
audit	Это аббревиатура: audit uid - идентификатор пользователя, использованный для входа в систему.
devmajor	Главный номер устройства (Device Major Number).
devminor	Вспомогательный номер устройства (Device Minor Number).
egid	Действительный идентификатор группы.
euid	Действительный идентификатор пользователя.
exit	Значение, возвращаемое системным вызовом при выходе.
fsgid	Идентификатор группы, применяемый к файловой системе.
fsuid	Идентификатор пользователя, применяемый к файловой системе.
gid	Идентификатор группы.

Поле сравнения	Описание
inode	Номер.
inode key	Альтернативный способ установить ключ фильтрации. Смотри выше описание опции «-k».
msgtype	Используется для проверки совпадения с числом, описывающим тип сообщения. Может быть использован только в списке exclude.
<obj_user>	Имя пользователя-владельца ресурса (в контексте SELinux).
<obj_role>	Роль ресурса (в контексте SELinux).
<obj_type>	Тип ресурса (в контексте SELinux).
<obj_lev_low>	Нижний уровень ресурса (в контексте SELinux).
<obj_lev_high>	Верхний уровень ресурса (в контексте SELinux).
path	Полный путь к файлу для точки наблюдения. Смотри ниже описание опции «-w». Может быть использован только в списке exit.
perm	Фильтр прав доступа для файловых операций. Смотри выше описание опции «-p». Может быть использован только в списке exit.
pers	Персональный номер операционной системы.
pid	Идентификатор процесса.
ppid	Идентификатор родительского процесса.
<subj_user>	Имя пользователя-владельца процесса (в контексте SELinux).
<subj_role>	Роль процесса (в контексте SELinux).
<subj_type>	Тип процесса (в контексте SELinux).
<subj_sen>	Чувствительность процесса (в контексте SELinux).
<subj_clr>	Допуск процесса (в контексте SELinux).
sgid	Установленный идентификатор группы.
success	Если значение, возвращаемое системным вызовом, больше либо равно 0, данный объект будет равен «true/yes», иначе «false/no». При создании правила используйте 1 вместо «true/yes» и 0 вместо «false/no».
suid	Установленный идентификатор пользователя.
uid	Идентификатор пользователя.

Поле сравнения	Описание
<code>-w &lt;путь&gt;</code>	Добавить точку наблюдения за файловым объектом, находящимся по указанному пути. Вы не можете добавлять точку наблюдения к каталогу верхнего уровня - это запрещено ядром. Групповые символы (wildcards) также не могут быть использованы, попытки их использования будут генерировать предупреждающее сообщение. Внутренне точки наблюдения реализованы как слежение за inode. Таким образом, если вы установите точку наблюдения за каталогом, вы увидите файловые события, которые в действительности будут означать обновления метаданных этой inode, и вы можете не увидеть событий, непосредственно связанных с файлами. Если вам необходимо следить за всеми файлами в каталоге, рекомендуется создавать индивидуальную точку наблюдения для каждого файла. В противоположность к правилам аудита системных вызовов, точки наблюдения не оказывают влияния на производительность, связанную с количеством правил посылаемых в ядро.
<code>-W &lt;путь&gt;</code>	Удалить точку наблюдения за файловым объектом, находящимся по указанному пути.

Примеры:

- Увидеть все системные вызовы, используемые определенным процессом:

```
auditctl -a entry,always -S all -F pid=1005
```

- Увидеть все файлы, открытые определенным пользователем:

```
auditctl -a exit,always -S open -F auid=510
```

- Увидеть неудачные попытки вызова системной функции «open»:

```
auditctl -a exit,always -S open -F success!=0
```

### Утилита aureport

Утилита aureport - это инструмент, который генерирует итоговые отчёты на основе логов службы аудита. aureport может также принимать данные со стандартного ввода (stdin) до тех пор, пока на входе будут необработанные данные логов.

В шапке каждого отчёта для каждого столбца есть заголовок - это облегчает понимание данных. Все отчёты, кроме основного итогового отчёта, содержат номера событий аудита. Используя их, вы можете найти полные данные о событии с помощью «ausearch -a <номер\_события>».

Если в отчёте слишком много данных, можно задать время начала и время окончания для уточнения временного промежутка. Отчёты, генерируемые

аугерорт, могут быть использованы как исходный материал для получения более развёрнутых отчётов.

Основные опции, используемые утилитой аугерорт, приведены в таблице.

Опция	Значение опции
-au, --auth	Отчёт о всех попытках аутентификации.
-a, --avc	Отчёт о всех авс сообщениях.
-c, --config	Отчёт о изменениях конфигурации.
-cr, --crypto	Отчёт о событиях, связанных с шифрованием.
-e, --event	Отчёт о событиях.
-f, --file	Отчёт о файлах.
--failed	Для обработки в отчётах выбирать только неудачные события. По умолчанию показываются и удачные и неудачные события.
-h, --host	Отчёт о хостах.
-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 аугерорт. Т.е. если вы переименовали учётные записи пользователей или не имеете таких же учётных записей на вашей машине, то вы можете получить результаты, вводящие в заблуждение.
-if, --input <файл>	Использовать указанный файл вместо логов аудита. Это может быть полезно при анализе логов с другой машины или при анализе частично сохранённых логов.
-l, --login	Отчёт о попытках входа в систему.
-m, --mods	Отчёт об изменениях пользовательских учётных записей.
-ma, --mac	Отчёт о событиях в системе, обеспечивающей мандатное управление доступом - Mandatory Access Control (MAC).
-p, --pid	Отчёт о процессах.
-r, --response	Отчёт о реакциях на аномальные события.
-s, --syscall	Отчёты о системных вызовах.
--success	Для обработки в отчётах выбирать только удачные события. По умолчанию показываются и удачные и неудачные события.
--summary	Генерировать итоговый отчёт, который даёт информацию только о количестве элементов в том или ином отчёте. Такой режим есть не у всех отчётов.
-t, --log	Этот параметр генерирует отчёт о временных рамках каждого отчёта.

Опция	Значение опции
-te, --end <дата> <время>	<p>Искать события, которые произошли раньше (или во время) указанной временной точки. Формат даты и времени зависит от ваших региональных настроек. Если дата не указана, то подразумевается текущий день (today). Если не указано время, то подразумевается текущий момент (now). Используйте 24-часовую нотацию времени, а не АМ/РМ. Например, дата может быть задана как 10/24/2005, а время - как 18:00:00.</p> <p>Вы можете также использовать ключевые слова: now, recent, today, yesterday, this-week, this-month, this-year. today означает первую секунду после полуночи текущего дня. recent - 10 минут назад. yesterday - первую секунду после полуночи предыдущего дня. this-week означает первую секунду после полуночи первого дня текущей недели, первый день недели определяется из ваших региональных настроек. this-month означает первую секунду после полуночи первого числа текущего месяца. this-year означает первую секунду после полуночи первого числа первого месяца текущего года.</p>
-tm, --terminal	<p>Отчёт о терминалах.</p>
-ts, --start <дата> <время>	<p>Искать события, которые произошли после (или во время) указанной временной точки. Формат даты и времени зависит от ваших региональных настроек. Если дата не указана, то подразумевается текущий день (today). Если не указано время, то подразумевается полночь (midnight). Используйте 24-часовую нотацию времени, а не АМ/РМ. Например, дата может быть задана как 10/24/2005, а время - как 18:00:00.</p> <p>Вы можете также использовать ключевые слова: now, recent, today, yesterday, this-week, this-month, this-year. today означает первую секунду после полуночи текущего дня. recent - 10 минут назад. yesterday - первую секунду после полуночи предыдущего дня. this-week означает первую секунду после полуночи первого дня текущей недели, первый день недели определяется из ваших региональных настроек. this-month означает первую секунду после полуночи первого числа текущего месяца. this-year означает первую секунду после полуночи первого числа первого месяца текущего года.</p>
-u, --user	<p>Отчёт о пользователях.</p>
-v, --version	<p>Вывести версию программы и выйти.</p>

### Утилита ausearch

Программа ausearch является инструментом поиска по журналу аудита. Утилита ausearch может также принимать данные со стандартного ввода (stdin) до тех пор, пока на входе будут необработанные данные логов. Все условия, указанные в параметрах, объединяются логическим «И». К примеру, при указании

«-m» и «-ui» в качестве параметров будут показаны события, соответствующие заданному типу и идентификатору пользователя.

Стоит отметить, что каждый системный вызов ядра из пользовательского пространства и возвращение данных в пользовательское пространство имеет один уникальный (для каждого системного вызова) идентификатор события.

Различные части ядра могут добавлять дополнительные записи. Например, в событие аудита для системного вызова «open» добавляется запись PATH с именем файла. ausearch показывает все записи события вместе. Это означает, что при запросе определенных записей результат может содержать записи SYSCALL.

Также помните, что не все типы записей содержат указанную информацию. Например, запись PATH не содержит имя узла или loginuid.

Основные опции, используемые утилитой ausearch, приведены в таблице.

Опция	Значение опции
-a, --event audit-event-id	Искать события с заданным идентификатором события. Сообщения обычно начинаются примерно так: msg=audit(1116360555.329:2401771). Идентификатор события - это число после «:». Все события аудита, связанные с одним системным вызовом, имеют одинаковый идентификатор.
-c, --comm comm-name	Искать события с заданным comm name. comm name - имя 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, --gidgroup-id	Искать события с заданным идентификатором группы или именем группы.
-h, --help	Справка.
-hn, --host host-name	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 учётные записи пользователей или не имеете таких же учётных 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 сохранённых логов.

Опция	Значение опции
-k, --key key-string	Искать события с заданным ключевым словом.
-m, --message message-type   comma-sep- message-type- list	Искать события с заданным типом. Вы можете указать список значений, разделённых 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. В списке значений этого параметра в качестве разделителя используются запятые и пробелы недопустимы.
-o, --object SE-Linux- context-string	Искать события с заданным контекстом (объектом).
-p, --pid process-id	Искать события с заданным идентификатором процесса.
-pp, --ppid parent- process-id	Искать события с заданным идентификатором родительского процесса.
-r, --raw	Необработанный вывод. Используется для извлечения записей для дальнейшего анализа.
-sc, --success syscall- name-or-value	Искать события с заданным системным вызовом. Вы можете указать его номер или имя. Если вы указали имя, оно будет проверено на машине, где запущен ausearch.
-se, --context SE-Linux- context-string	Искать события с заданным контекстом SELinux (stcontext/subject или tcontext/object).
-su, --subject SE-Linux- context-string	Искать события с заданным контекстом SELinux - scontext (subject).
-sv, --success success- value	Искать события с заданным флагом успешного выполнения. Допустимые значения: «yes» (успешно) и «no» (неудачно).

Опция	Значение опции
-te, --end [end-date] [end-time]	<p>Искать события, которые произошли раньше (или во время) указанной временной точки. Формат даты и времени зависит от ваших региональных настроек. Если дата не указана, то подразумевается текущий день (today). Если не указано время, то подразумевается текущий момент (now). Используйте 24-часовую нотацию времени, а не АМ/РМ. Например, дата может быть задана как 10/24/2005, а время - как 18:00:00.</p> <p>Вы можете также использовать ключевые слова: now, recent, today, yesterday, this-week, this-month, this-year. today означает первую секунду после полуночи текущего дня. recent - 10 минут назад. yesterday - первую секунду после полуночи предыдущего дня. this-week означает первую секунду после полуночи первого дня текущей недели, первый день недели определяется из ваших региональных настроек (см. localtime). this-month означает первую секунду после полуночи первого числа текущего месяца. this-year означает первую секунду после полуночи первого числа первого месяца текущего года.</p>
-ts, --start [start-date] [start-time]	<p>Искать события, которые произошли после (или во время) указанной временной точки. Формат даты и времени зависит от ваших региональных настроек. Если дата не указана, то подразумевается текущий день (today). Если не указано время, то подразумевается полночь (midnight). Используйте 24-часовую нотацию времени, а не АМ/РМ. Например, дата может быть задана как 10/24/2005, а время - как 18:00:00.</p> <p>Вы можете также использовать ключевые слова: now, recent, today, yesterday, this-week, this-month, this-year. today означает первую секунду после полуночи текущего дня. recent - 10 минут назад. yesterday - первую секунду после полуночи предыдущего дня. this-week означает первую секунду после полуночи первого дня текущей недели, первый день недели определяется из ваших региональных настроек. this-month означает первую секунду после полуночи первого числа текущего месяца. this-year означает первую секунду после полуночи первого числа первого месяца текущего года.</p>
-tm, --terminal terminal	<p>Искать события с заданным терминалом. Некоторые службы (такие как cron и atd) используют имя службы как имя терминала.</p>
-ua, --uid-all all-user-id	<p>Искать события, у которых любой из идентификатора пользователя, эффективного идентификатора пользователя или loginuid (auid) совпадают с заданным идентификатором пользователя.</p>

Опция	Значение опции
<code>-ue, --uid-effective effective-user-id</code>	Искать события с заданным эффективным идентификатором пользователя.
<code>-ui, --uid user-id</code>	Искать события с заданным идентификатором пользователя.
<code>-ul, --loginuid login-id</code>	Искать события с заданным идентификатором пользователя. Все программы, которые его используют, должны использовать <code>ram_loginuid</code> .
<code>-v, --verbose</code>	Показать версию и выйти.
<code>-w, --word</code>	Совпадение с полным словом. Поддерживается для имени файла, имени узла, терминала и контекста SELinux.
<code>-x, --executable executable</code>	Искать события с заданным именем исполняемой программы.

### Утилита `autrace`

Утилита `autrace` - это программа, которая добавляет правила аудита для того, чтобы следить за использованием системных вызовов в указанном процессе подобно тому, как это делает `strace`.

После добавления правил она запускает процесс с указанными аргументами. Результаты аудита будут либо в логах аудита (если служба аудита запущена), 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 `auditctl` – предупреждающее сообщение известит об этом.

Опции утилиты `autrace` приведены в таблице.

Опция	Значение опции
<code>-r</code>	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.

Примеры:

- Обычное использование программы:

```
autrace /bin/ls /tmp
ausearch --start recent -p 2442 -i
```

- Режим 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
```

### Графическая утилита просмотра журналов аудита

После запуска программы просмотра системных журналов отображается следующее окно (рисунок 6.1).

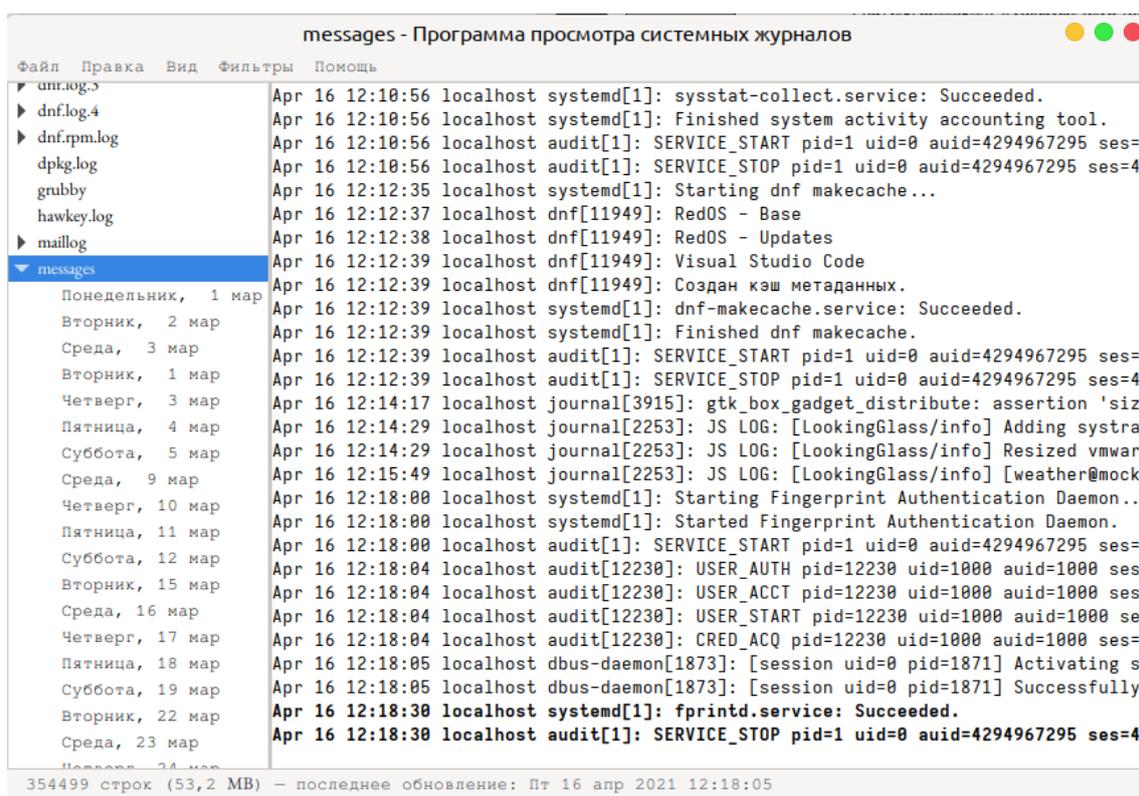


Рисунок 6.1 - Окно программы просмотра системных журналов

Для доступа к журналам аудита пользователь должен ввести пароль администратора. После первого запуска программы просмотра системных журналов приложение по умолчанию отображает несколько файлов журналов (такие, как `/var/log/messages`). Открытые логи (журналы) представлены в списке в левой части окна приложения. Выбранный из списка журнал отображается в главной части окна приложения.

По умолчанию программа просмотра системных журналов отображает изменения каждого открытого журнала, и любые изменения появляются автоматически в главном окне.

Заметьте, что программа просмотра системных журналов также позволяет вам открывать архивированные журналы (названия файлов которых оканчиваются на «.gz»).

Чтобы скопировать одну или более строк журнала в буфер обмена, просто выделите строки в главной части окна и выберите Правка ► Копировать.

Если вы хотите копировать весь журнал в буфер обмена, выберите его полностью, используя настройку Правка ► Выделить всё, затем выберите Правка ► Копировать.

Вы можете использовать программу просмотра системных журналов для мониторинга логов (журналов). По умолчанию, ко всем журналам, открытым в программе просмотра системных журналов, применяются текущие изменения. Если новые строки добавлены к журналу, просматриваемому с помощью программы просмотра системных журналов, наименование журнала выделится жирным начертанием шрифта в списке журналов. Если журнал отображается в настоящее время в главной части окна, новые линии появятся автоматически в конце журнала и, по истечении пяти секунд, наименование журнала снова вернётся к обычному начертанию в списке журналов.

Информация о журнале обычно отображена в строке состояния, включая:

- количество строк в журнале;
- размер журнала в байтах;
- дату последнего обновления (изменения) журнала.

Строка состояния может быть показана или скрыта через пункт меню Вид ► Строка состояния.

### Экспорт данных аудита

Для экспорта данных аудита для другого доверенного ИТ-продукта предлагается использовать сжатые архивные файлы с парольной защитой. Архив позволит значительно уменьшить объем передаваемых данных, а пароль защитит от несанкционированного раскрытия при передаче. Для сжатия журналов аудита необходимо использовать утилиту zip.

Zip - это утилита для сжатия и упаковки файлов и каталогов. Чтобы сжать файл или каталог с помощью команды zip, наберите в командной строке:

```
zip -r <имя_файла>.zip <каталог>
```

В этом примере <имя\_файла>.zip — создаваемый вами файл, а <каталог> — каталог, который будет помещён в новый zip-файл. Опция «-r» указывает, что все файлы из каталога <каталог> будут включены рекурсивно.

Установить пароль на архив можно с помощью ключа «-P», а ключ «-e» скроет пароль при вводе.

ОС, при соответствующей настройке, формирует ряд журналов аудита. Типы событий безопасности и места размещения соответствующих журналов приведены в таблице.

Событие	Журнал аудита
Запуск и завершение выполнения функций аудита	/var/log/audit/audit.log
Запись аудита для событий, связанных с истечением установленного администратором срока действия пароля	/var/log/secure

Событие	Журнал аудита
Запись аудита для событий, связанных с истечением установленного администратором срока действия идентификатора пользователя ОС (учетной записи)	/var/log/secure
Действия, предпринимаемые в ответ на возможные нарушения безопасности	/var/log/maillog
Все модификации конфигурации аудита, происходящие во время сбора данных аудита	/var/log/audit/audit.log
Блокирование учётной записи в результате превышения максимального числа неуспешных попыток входа в систему	/var/log/secure
Все модификации политики аудита	/var/log/audit/audit.log
Все модификации значений атрибутов безопасности, используемых для смены начальной аутентификационной информации пользователя ОС после однократного использования	/var/log/secure
Все модификации аутентификационной информации	/var/log/secure
Полнотекстовая запись привилегированных команд (команд, управляющих системными функциями)	/var/log/audit/audit.log
Применение механизма восстановления информации	/var/log/messages
Изменение настроек механизмов уничтожения (стирания) данных	/var/log/audit/audit.log
Сбои в работе механизма изоляции процессов	/var/log/messages
Попытки установки внешних модулей уровня ядра, не проверенных разработчиком (производителем), или внешних модулей уровня ядра с нарушенной целостностью	/var/log/audit/audit.log
Попытки запуска компонентов программного обеспечения, целостность которых была нарушена, и попытки запуска компонентов программного обеспечения, произведённых в нарушение установленных правил запуска компонентов программного обеспечения	/var/log/audit/audit.log
Чтение информации из записей аудита, неуспешные попытки читать информацию из записей аудита	/var/log/audit/audit.log
Предпринимаемые действия после превышения порога заполнения журнала аудита, предпринимаемые действия при сбое хранения журнала аудита	/var/log/messages
Все запросы на выполнение операций на объекте, на который распространяется политика дискреционного или ролевого доступа	/var/log/audit/audit.log
Все попытки экспортировать информацию	/var/log/audit/audit.log

Событие	Журнал аудита
Все решения по запросам на сетевые потоки при использовании фильтрации сетевых потоков	/var/log/messages
Отклонение или принятие любого проверенного пароля при проверке его на сложность/заданные метрики	/var/log/secure
Все случаи использования механизма аутентификации, результат действия каждого активизированного механизма вместе с итоговым решением	/var/log/secure
Все случаи использования механизма идентификации пользователя, включая представленный идентификатор пользователя	/var/log/secure
Успешное или неуспешное связывание атрибутов безопасности пользователя с субъектом	/var/log/secure
Назначение срока действия для атрибута и действия, предпринятые по истечении назначенного срока.	/var/log/secure; /var/log/audit/audit.log
Модификация группы пользователей	/var/log/audit/audit.log
Использование функций управления	/var/log/messages
Изменения внутреннего представления времени	/var/log/messages
Выполнение и результаты самотестирования	/var/log/messages
Тип сбоя или прерывания обслуживания	/var/log/messages
Все операции ОС, прерванные из-за сбоя	/var/log/messages
Все попытки использования функции распределения ресурсов с учетом приоритетности обслуживания	/var/log/audit/audit.log
Все обращения к функциям распределения ресурсов	/var/log/audit/audit.log
Отклонение нового сеанса, основанное на ограничении числа параллельных сеансов	/var/log/secure
Все попытки разблокирования интерактивного сеанса	/var/log/secure
Завершение интерактивного сеанса механизмом блокирования сеанса	/var/log/messages

Записи журналов аудита имеют следующий вид:

Журнал аудита	Пример записи события безопасности
/var/log/audit/ audit.log	<pre> type=DAEMON_START msg=audit(1505824570.753:4329): op=start ver=2.6.5 format=raw kernel=4.9.30-1.el7.x86_64 aid=4294967295 pid=614 subj=system_u:system_r:auditd_t:s0 res=success type=SERVICE_START msg=audit(1505824570.773:6): pid=1 uid=0 aid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg='unit=rngd comm="systemd" exe="/usr/lib/systemd/s </pre>
/var/log/secure	<pre> Oct 11 09:51:01 redos login[4682]: LOGIN ON tty2 BY ivanov Oct 11 09:56:40 redos vlock[5049]: pam_unix(vlock:auth): authentication failure; logname= uid=1001 euid=1001 tty=pts/0 ruser= rhost= user=ivanov </pre>
/var/log/maillog	<pre> Oct 17 10:47:11 redos postfix/cleanup[9004]: E66AE400BE: message-id=&lt;20171017074711.E66AE400BE@redos. localdomain&gt; Oct 17 10:47:11 redos postfix/qmgr[2780]: E66AE400BE: from=&lt;root@redos.local domain&gt;, size=496, nrcpt=1 (queue active) </pre>
/var/log/messages	<pre> Oct 11 09:49:38 redos systemd[1]: Starting Local File Systems (Pre). Oct 11 09:49:38 redos systemd[1]: Mounting /mnt/test_disk... Oct 11 09:49:38 redos kernel: EXT4-fs (sdb1): mounted filesystem with ordered data mode. Opts: (null) </pre>

## 6.4 Права доступа к файлам и каталогам

РЕД ОС — система многопользовательская, поэтому вопрос об организации разграничения доступа к файлам и каталогам является одним из существенных вопросов, которые должна решать операционная система.

В основе механизмов разграничения доступа лежат имена пользователей и имена групп пользователей. В РЕД ОС каждый пользователь имеет уникальное имя, под которым он входит в систему (логинится). Кроме того, в системе создаётся некоторое число групп пользователей, причём каждый пользователь может быть включён в одну или несколько групп. Создаёт и удаляет группы суперпользователь, он же может изменять состав участников той или иной группы. Члены разных групп могут иметь разные права по доступу к файлам, например, группа администраторов может иметь больше прав, чем группа программистов.

В индексном дескрипторе каждого файла записаны имя так называемого владельца файла и группы, которая имеет права на этот файл. Первоначально,

при создании файла его владельцем объявляется тот пользователь, который этот файл создал. Точнее — тот пользователь, от чьего имени запущен процесс, создающий файл. Группа тоже назначается при создании файла — по идентификатору группы процесса, создающего файл. Владельца и группу файла можно поменять в ходе дальнейшей работы с помощью команд «chown» и «chgrp».

Выполним команду «ls -l». Но зададим ей в качестве дополнительного параметра имя конкретного файла, например, файла, задающего саму команду ls.

```
ls -l /bin/ls
```

```
-rwxr-xr-x 1 root root 49940 Sep 12 1999 /bin/ls
```

В данном случае владельцем файла является пользователь root и группа root. Но нас сейчас в выводе этой команды больше интересует первое поле, определяющее тип файла и права доступа к файлу. Это поле в приведённом примере представлено цепочкой символов «-rwxr-xr-x». Эти символы можно условно разделить на 4 группы.

Первая группа, состоящая из единственного символа, определяет тип файла. Этот символ в соответствии с возможными типами файлов может принимать такие значения:

- - — обычный файл;
- d — каталог;
- b — файл блочного устройства;
- c — файл символьного устройства;
- s — доменное гнездо (socket);
- p — именованный канал (pipe);
- l — символическая ссылка (link).

Далее следуют три группы по три символа, которые и определяют права доступа к файлу соответственно для владельца файла, для группы пользователей, которая сопоставлена данному файлу, и для всех остальных пользователей системы. В нашем примере права доступа для владельца определены как «rwx», что означает, что владелец (root) имеет право читать файл (r), производить запись в этот файл (w) и запускать файл на выполнение (x). Замена любого из этих символов прочерком будет означать, что пользователь лишается соответствующего права. В том же примере мы видим, что все остальные пользователи (включая и тех, которые вошли в группу root) лишены права записи в этот файл, т. е. не могут файл редактировать и вообще как-то изменять.

Права доступа и информация о типе файла хранятся в индексных дескрипторах в отдельной структуре, состоящей из двух байтов, т. е. из 16 бит. Четыре бита из этих 16-ти отведены для кодированной записи о типе файла. Следующие три бита задают особые свойства исполняемых файлов. И, наконец, оставшиеся 9 бит определяют права доступа к файлу. Эти 9 бит разделяются на 3 группы по три бита. Первые три бита задают права пользователя, следующие три бита — права группы, последние 3 бита определяют права всех остальных пользователей (т. е. всех пользователей, за исключением владельца файла и группы файла).

При этом, если соответствующий бит имеет значение «1», то право предоставляется, а если он равен «0», то право не предоставляется. В символьной форме записи прав единица заменяется соответствующим символом (r, w или x), а 0 представляется прочерком.

Право на чтение (r) файла означает, что пользователь может просматривать содержимое файла с помощью различных команд просмотра, например, командой «more» или с помощью любого текстового редактора. Но, отредактировав содержимое файла в текстовом редакторе, вы не сможете сохранить изменения в файле на диске, если не имеете права на запись (w) в этот файл. Право на выполнение (x) означает, что вы можете загрузить файл в память и попытаться запустить его на выполнение как исполняемую программу. Конечно, если в действительности файл не является программой (или скриптом shell), то запустить этот файл на выполнение не удастся, но, с другой стороны, даже если файл действительно является программой, но право на выполнение для него не установлено, то он тоже не запустится.

Если выполнить ту же команду «ls -l», но в качестве последнего аргумента ей указать не имя файла, а имя каталога, мы увидим, что для каталогов тоже определены права доступа, причём они задаются теми же самыми символами rwx. Например, выполнив команду «ls -l /», мы увидим, что каталогу bin соответствует строка:

```
drwxr-xr-x 2 root root 2048 Jun 21 21:11 bin
```

Естественно, что по отношению к каталогам трактовка понятий «право на чтение», «право на запись» и «право на выполнение» несколько изменяется. Право на чтение по отношению к каталогам легко понять, если вспомнить, что каталог — это просто файл, содержащий список файлов в данном каталоге. Следовательно, если вы имеете право на чтение каталога, то вы можете просматривать его содержимое (этот самый список файлов в каталоге). Право на запись тоже понятно — имея такое право, вы сможете создавать и удалять файлы в этом каталоге, т. е. просто добавлять в каталог или удалять из него запись, содержащую имя какого-то файла и соответствующие ссылки. Право на выполнение в данном случае означает право переходить в этот каталог. Если вы, как владелец, хотите дать доступ другим пользователям на просмотр какого-то файла в своём каталоге, вы должны дать им право доступа в каталог, т. е. дать им «право на выполнение каталога». Более того, надо дать пользователю право на выполнение для всех каталогов, стоящих в дереве выше данного каталога. Поэтому в принципе для всех каталогов по умолчанию устанавливается право на выполнение как для владельца и группы, так и для всех остальных пользователей. И, уж если вы хотите закрыть доступ в каталог, то лишите всех пользователей (включая группу) права входить в этот каталог.

После прочтения предыдущего абзаца может показаться, что право на чтение каталога не даёт ничего нового по сравнению с правом на выполнение. Однако разница в этих правах все же есть. Если задать только право на выполнение, вы сможете войти в каталог, но не увидите там ни одного файла (этот эффект особенно наглядно проявляется в том случае, если вы пользуетесь каким-то файловым менеджером, например, программой Midnight Commander). Если вы

имеете право доступа в каком-то из подкаталогов этого каталога, то вы можете перейти в него (командой `cd`), но, как говорится «вслепую», по памяти, потому что списка файлов и подкаталогов текущего каталога вы не увидите.

Алгоритм проверки прав пользователя при обращении к файлу можно описать следующим образом. Система вначале проверяет, совпадает ли имя пользователя с именем владельца файла. Если эти имена совпадают (т. е. владелец обращается к своему файлу), то проверяется, имеет ли владелец соответствующее право доступа: на чтение, на запись или на выполнение (не удивляйтесь, суперпользователь может лишить некоторых прав и владельца файла). Если право такое есть, то соответствующая операция разрешается. Если же нужного права владелец не имеет, то проверка прав, предоставляемых через группу или через группу атрибутов доступа для остальных пользователей, уже даже не проверяются, а пользователю выдаётся сообщение о невозможности выполнения затребованного действия.

Если имя пользователя, обращающегося к файлу, не совпадает с именем владельца, то система проверяет, принадлежит ли владелец к группе, которая сопоставлена данному файлу (далее будем просто называть ее группой файла). Если принадлежит, то для определения возможности доступа к файлу используются атрибуты, относящиеся к группе, а на атрибуты для владельца и всех остальных пользователей внимания не обращается. Если же пользователь не является владельцем файла и не входит в группу файла, то его права определяются атрибутами для остальных пользователей. Таким образом, третья группа атрибутов, определяющих права доступа к файлу, относится ко всем пользователям, кроме владельца файла и пользователей, входящих в группу файла.

### 6.4.1 `chmod`

Для изменения прав доступа к файлу используется команда `chmod`. Ее можно использовать в двух вариантах. В первом варианте вы должны явно указать, кому какое право даёте или кого этого права лишаете:

```
chmod wXr <имя_файла>
```

где вместо символа `<w>` подставляется:

- либо символ «`u`» (т. е. пользователь, который является владельцем);
- либо «`g`» (группа);
- либо «`o`» (все пользователи, не входящие в группу, которой принадлежит данный файл);
- либо «`a`» (все пользователи системы, т. е. и владелец, и группа, и все остальные).

Вместо `<X>` ставится:

- либо «`+`» (предоставить право);
- либо «`-`» (лишить соответствующего права);
- либо «`=`» (установить указанные права вместо имеющихся).

Вместо `<r>` — символ, обозначающий соответствующее право:

- «`r`» (чтение);

- «w» (запись);
- «x» (выполнение).

Вот несколько примеров использования команды `chmod`:

- Предоставление всем пользователям системы прав на выполнение данного файла:

```
chmod a+x <имя_файла>
```

- Удаление права на чтение и запись для всех, кроме владельца файла:

```
chmod go-rw <имя_файла>
```

- Установка всем прав на чтение, запись и выполнение:

```
chmod ugo+rwx <имя_файла>
```

Если опустить указание на то, кому предоставляется данное право, то подразумевается, что речь идёт вообще обо всех пользователях, т. е. вместо:

```
chmod a+x <имя_файла>
```

можно записать просто:

```
chmod +x <имя_файла>
```

Второй вариант задания команды `chmod` (он используется чаще) основан на цифровом представлении прав. Для этого мы кодируем символ «r» цифрой 4, символ «w» — цифрой 2, а символ «x» — цифрой 1. Для того, чтобы предоставить пользователям какой-то набор прав, надо сложить соответствующие цифры. Получив, таким образом, нужные цифровые значения для владельца файла, для группы файла и для всех остальных пользователей, задаём эти три цифры в качестве аргумента команды `chmod` (ставим эти цифры после имени команды перед вторым аргументом, который задаёт имя файла). Например, если надо дать все права владельцу ( $4+2+1=7$ ), право на чтение и запись — группе ( $4+2=6$ ), и не давать никаких прав остальным, то следует дать такую команду:

```
chmod 760 <имя_файла>
```

Если вы знакомы с двоичным кодированием восьмеричных цифр, то вы поймёте, что цифры после имени команды в этой форме ее представления есть ни что иное, как восьмеричная запись тех самых 9 бит, которые задают права для владельца файла, группы файла и для всех пользователей.

Выполнять смену прав доступа к файлу с помощью команды `chmod` может только сам владелец файла или суперпользователь. Для того, чтобы иметь возможность изменить права группы, владелец должен дополнительно быть членом той группы, которой он хочет дать права на данный файл.

Надо рассказать ещё о трёх возможных атрибутах файла, устанавливаемых с помощью той же команды `chmod`. Это те самые атрибуты для исполняемых файлов, которые в индексном дескрипторе файла в двухбайтовой структуре,

определяющей права на файл, занимают позиции 5-7, сразу после кода типа файла.

Первый из этих атрибутов — так называемый «бит смены идентификатора пользователя». Смысл этого бита состоит в следующем.

Обычно, когда пользователь запускает некоторую программу на выполнение, эта программа получает те же права доступа к файлам и каталогам, которые имеет пользователь, запустивший программу. Если же установлен «бит смены идентификатора пользователя», то программа получит права доступа к файлам и каталогам, которые имеет владелец файла программы (таким образом, рассматриваемый атрибут лучше называть «битом смены идентификатора владельца»). Это позволяет решать некоторые задачи, которые иначе было бы трудно выполнить. Самый характерный пример — команда смены пароля `passwd`. Все пароли пользователей хранятся в файле `/etc/passwd`, владельцем которого является суперпользователь `root`. Поэтому программы, запущенные обычными пользователями, в том числе команда `passwd`, не могут производить запись в этот файл. А значит, пользователь как бы не может менять свой собственный пароль. Но для файла `/usr/bin/passwd` установлен «бит смены идентификатора владельца», каковым является пользователь `root`. Следовательно, программа смены пароля `passwd` запускается с правами `root` и получает право записи в файл `/etc/passwd` (уже средствами самой программы обеспечивается то, что пользователь может изменить только одну строку в этом файле).

Установить «бит смены идентификатора владельца» может суперпользователь с помощью команды

```
chmod +s <имя_файла>
```

Аналогичным образом работает «бит смены идентификатора группы».

Еще один возможный атрибут исполняемого файла — это «бит сохранения задачи» или «sticky bit» (дословно — «бит прилипчивости»). Этот бит указывает системе, что после завершения программы надо сохранить ее в оперативной памяти. Удобно включить этот бит для задач, которые часто вызываются на выполнение, так как в этом случае экономится время на загрузку программы при каждом новом запуске. Этот атрибут был необходим на старых моделях компьютеров. На современных быстродействующих системах он используется редко.

Если используется цифровой вариант задания атрибутов в команде `chmod`, то цифровое значение этих атрибутов должно предшествовать цифрам, задающим права пользователя:

```
chmod 4775 <имя_файла>
```

При этом веса этих битов для получения нужного суммарного результата задаются следующим образом:

- 4 — «бит смены идентификатора пользователя»;
- 2 — «бит смены идентификатора группы»;
- 1 — «бит сохранения задачи (sticky bit)».

Если какие-то из этих трёх битов установлены в 1, то несколько изменяется

вывод команды «ls -l» в части отображения установленных атрибутов прав доступа. Если установлен в 1 «бит смены идентификатора пользователя», то символ «x» в группе, определяющей права владельца файла, заменяется символом «s». Причём, если владелец имеет право на выполнение файла, то символ «x» заменяется на маленькое «s», а если владелец не имеет права на выполнение файла (например, файл вообще не исполняемый), то вместо «x» ставится «S». Аналогичные замены имеют место при задании «бита смены идентификатора группы», но заменяется символ «x» в группе атрибутов, задающих права группы. Если равен 1 «бит сохранения задачи (sticky bit)», то заменяется символ «x» в группе атрибутов, определяющей права для всех остальных пользователей, причём «x» заменяется символом «t», если все пользователи могут запускать файл на выполнение, и символом «T», если они такого права не имеют.

Таким образом, хотя в выводе команды «ls -l» не предусмотрено отдельных позиций для отображения значений битов смены идентификаторов и бита сохранения задачи, соответствующая информация выводится. Вот небольшой пример того, как это будет выглядеть:

```
ls -l prim1
```

```
-rwSrwsrwT 1 kos root 12 Dec 18 23:17 prim1
```

### 6.4.2 umask

umask (от англ. user file creation mode mask — маска режима создания пользовательских файлов) — функция среды POSIX, изменяющая права доступа, которые присваиваются новым файлам и директориям по умолчанию. Права доступа файлов, созданных при конкретном значении umask, вычисляются при помощи следующих побитовых операций (umask обычно устанавливается в восьмеричной системе счисления): побитовое «И» между унарным дополнением аргумента (используя побитовое «НЕ») и режимом полного доступа.

Фактически, umask указывает, какие биты следует сбросить в выставляемых правах на файл — каждый установленный бит umask запрещает выставление соответствующего бита прав. Исключением из этого запрета является бит исполняемости, который для обычных файлов зависит от создающей программы (трансляторы ставят бит исполняемости на создаваемые файлы, другие программы — нет), а для каталогов следует общему правилу. umask 0 означает, что следует (можно) выставить все биты прав (rwxrwxrwx), umask 777 запрещает выставление любых прав.

Допустим, что значение umask равняется 174, тогда каждый новый файл будет иметь права доступа 602, а каждая новая директория 603.

### 6.4.3 chown

chown (от англ. change owner) — утилита, изменяющая владельца и/или группу для указанных файлов. В качестве имени владельца/группы берётся первый аргумент, не являющийся опцией. Если задано только имя пользователя (или числовой идентификатор пользователя), то данный пользователь становится

владельцем каждого из указанных файлов, а группа этих файлов не изменяется. Если за именем пользователя через двоеточие следует имя группы (или числовой идентификатор группы), без пробелов между ними, то изменяется также и группа файла.

Синтаксис:

```
chown [-cfhvR] [--dereference] [--reference=rfile] <пользователь>
[:<группа>] <файл>...
```

Основные опции, используемые утилитой `chown`, приведены в таблице.

Опция	Значение опции
<code>-c, --changes</code>	Подробно описывать действие для каждого файла, владелец которого действительно изменяется.
<code>-f, --silent, --quiet</code>	Не выдавать сообщения об ошибках для файлов, чей владелец не может быть изменён.
<code>-h, --no-dereference</code>	Работать с самими символьными ссылками, а не с файлами, на которые они указывают. Данная опция доступна только если имеется системный вызов <code>lchown</code> .
<code>-R, --recursive</code>	Рекурсивное изменение владельца каталогов и их содержимого.
<code>-v, --verbose</code>	Подробное описание действия (или отсутствия действия) для каждого файла.
<code>--dereference</code>	Изменить владельца файла, на который указывает символьная ссылка, вместо самой символьной ссылки.
<code>--reference=rfile</code>	Изменить владельца файла на того, который является владельцем файла.

#### 6.4.4 ACL

ACL (Access Control List - Список Контроля Доступа) предоставляет расширенный и более гибкий механизм распределения прав файловых систем. Он предназначен для расширения прав доступа к файлам. ACL позволяет устанавливать разрешения любым пользователям или группам для различных файловых ресурсов.

Чтобы включить ACL, файловая система должна быть смонтирована с опцией «`acl`». Используйте «`fstab`» для постоянного монтирования с данной опцией.

Для изменения прав ACL используйте команду «`setfacl`».

Добавить разрешения для пользователя (<user> здесь имя пользователя или его ID):

```
setfacl -m "u:<user>:permissions" <file/dir>
```

Добавить разрешения для группы (<group> здесь имя группы или её ID):

```
setfacl -m "g:<group>:permissions" <file/dir>
```

Все файлы и каталоги при создании будут наследовать записи ACL родительского каталога:

```
setfacl -dm "entry" <dir>
```

Удалить определённую ACL запись:

```
setfacl -x "entry" <file/dir>
```

Удалить все ACL записи:

```
setfacl -b <file/dir>
```

Посмотреть права ACL:

```
getfacl <file/dir>
```

Удаление всех записей расширения ACL:

```
setfacl -b abc
```

Проверка разрешений:

```
getfacl abc
```

Знак «+»(плюс) в выводе команды «ls -l», который следует за правами Unix, указывает на использование ACL.

```
ls -l /dev/audio
```

```
crw-rw----+ 1 root audio 14, 4 nov. 9 12:49 /dev/audio
```

```
getfacl /dev/audio
```

```
getfacl: Removing leading '/' from absolute path names
# file: dev/audio
# owner: root
# group: audio
user::rw-
user:solstice:rw-
group::rw-
mask::rw-
other::---
```

Поиск файлов с правами ACL:

```
getfacl -R -s -p <dir> | sed -n 's/^# file: //p'
```

Данная команда ищет в указанном каталоге и его подкаталогах все файлы и директории, которые имеют права ACL.

### 6.4.5 Chattr и lsattr

chattr — изменяет атрибуты файлов на файловых системах ext3, ext4.

Синтаксис:

```
chattr [ -RV ] [ -v <версия> ] [ <атрибуты> ] <файлы>...
```

Основные опции утилиты chattr приведены в таблице.

Опция	Значение опции
-R	Рекурсивно изменять атрибуты каталогов и их содержимого. Все найденные символические ссылки будут игнорироваться
-v	Выводит более полную выводимую информацию и версию программы chattr
-f	Отключить вывод большинства ошибок
-p <проект>	Установить номер проекта
-v <версия>	Установить номер версии/генерации файла

Формат символьного режима:

```
+--[ASacDdIijsTtu]
```

Оператор «+» обозначает добавление указанных атрибутов к существующим; «-» обозначает их снятие; «=» обозначает установку только этих атрибутов файлам.

Символы «ASacDdijisu» указывают на новые атрибуты файлов:

Символ	Значение символа
a (append only)	Файл может быть открыт только в режиме до записи.
A (no atime updates)	Не обновлять поле atime (время последнего доступа) файла. Уменьшает количество операций записи на устройство.
c (compressed)	Файл записан на диск с использованием сжатия.
C (no copy-on-write)	Отключение режима «Copy-on-write» для указанного файла.
d (no dump)	Отключает создание архивной копии файла программой dump.

Символ	Значение символа
D (synchronous directory updates)	Включает синхронную запись изменений в данном каталоге. Это эквивалентно опции <code>dirsync</code> при монтировании файловой системы.
e (extent format)	Включает использование <code>extent</code> при выделении места на устройстве. Атрибут не может быть отключён с помощью <code>chattr</code> .
E	Атрибут экспериментальных методов сжатия. Атрибут не может быть установлен или снят с помощью <code>chattr</code> .
i (immutable)	Указывает, что файл защищен от изменений: не может быть удалён или переименован, никакая ссылка (жёсткая) не может быть создана на этот файл, никакие данные не могут быть записаны в файл.
I	Указывает что указанный каталог проиндексирован с помощью хеш-дерева.
j (data journalling)	Все данные файла перед записью будут полностью записаны в журнал <code>ext3/ext4</code> , несмотря на опции монтирования « <code>data=ordered</code> » или « <code>data=writeback</code> ». В режиме « <code>data=journal</code> » бессмыслен.
P (project hierarchy)	Указывает, что каталог с вложенными файлами является иерархической структурой проекта.
s (secure deletion)	Атрибут защищённого удаления файла, перед удалением все содержимое файла полностью затирается «00».
S (synchronous updates)	Атрибут синхронной записи для данного файла, аналогичен опции монтирования « <code>sync</code> » файловой системы.
t (no tail-merging)	Отключает метод <code>tail-merging</code> для файла.
T (top of directory hierarchy)	Указывает что каталог является головой иерархии каталогов.
u (undeletable)	Указывает системе, что при удалении файла его содержимое должно быть сохранено с возможностью дальнейшего восстановления.

`lsattr` - выводит атрибуты файла расширенной файловой системы.

Синтаксис:

```
lsattr [ -RVadv ] <файлы>
```

lsattr выводит атрибуты файла, которые могли быть установлены ранее командой chattr.

Основные опции утилиты lsattr приведены в таблице.

Опция	Значение опции
-R	Рекурсивно выводит атрибуты каталогов и их содержимого.
-V	Выводит версию программы.
-a	Выводит информацию по всем файлам в каталогах, включая скрытые файлы, чьи имена начинаются с «.».
-d	Отображает имена каталогов так же, как и остальные обычные файлы (взамен вывода списков их содержимого).
-v	Выводит версию или номер поколения файла.

## 6.5 Systemd – управление компонентами ОС

Systemd – менеджер системы и сервисов в операционной системе РЕД ОС.

Systemd реализует концепцию юнитов systemd. Юниты представлены конфигурационными файлами, размещёнными в одной из директорий:

- /usr/lib/systemd/system/ – юниты из установленных пакетов RPM;
- /run/systemd/system/ – юниты, созданные в рантайме. Этот каталог приоритетнее каталога с установленными юнитами из пакетов;
- /etc/systemd/system/ – юниты, созданные и управляемые системным администратором. Этот каталог приоритетнее каталога юнитов, созданных в рантайме.

Юниты содержат информацию о системных сервисах, прослушиваемых сокетах, сохраненных снимках состояний системы и других объектах, относящихся к системе инициализации.

Типы юнитов systemd:

- .service – системный сервис;
- .target – группа юнитов systemd;
- .automount – точка автомонтирования файловой системы;
- .device – файл устройства, распознанного ядром;
- .mount – точка монтирования файловой системы;
- .path – файл или директория в файловой системе;
- .scope – процесс, созданный извне;
- .slice – группа иерархически организованных юнитов, управляющая системными процессами;
- .snapshot – сохранённое состояние менеджера systemd;
- .socket – сокет межпроцессного взаимодействия;
- .swap – своп-устройство или своп-файл (файл подкачки);
- .timer – таймер systemd.

Во время загрузки systemd прослушивает сокеты для всех системных серви-

сов, поддерживает этот тип активации и передаёт сокеты этим сервисам сразу после старта сервисов. Это позволяет `systemd` не только запускать сервисы параллельно, но также дает возможность перезапускать сервисы без потери любых отправленных им сообщений, пока сервисы были недоступны. Соответствующий сокет остается доступным и все сообщения выстраиваются в очередь.

Системные сервисы, использующие D-Bus для межпроцессного взаимодействия, могут быть запущены по требованию, когда клиентское приложение пытается связаться с ними.

Системные сервисы, поддерживающие активацию, основанную на устройствах, могут быть запущены, когда определённый тип оборудования подключается или становится доступным.

Системные сервисы могут поддерживать этот вид активации, если изменяется состояние папки или директории.

Система может сохранять состояние всех юнитов и восстанавливать предыдущее состояние системы.

`Systemd` отслеживает и управляет точками монтирования и автосмонтирования.

Агрессивная параллелизация `Systemd` запускает системные сервисы параллельно из-за использования активации, основанной на сокетах. В комбинации с сервисами, поддерживающими активацию по требованию, параллельная активация значительно уменьшает время загрузки системы.

До активации и деактивации юнитов `systemd` вычисляет их зависимости, создает временную транзакцию и проверяет целостность этой транзакции. Если транзакция не целостная, `systemd` автоматически пытается исправить ее и удалить не требующиеся задания из нее до формирования сообщения об ошибке.

`SystemD` полностью поддерживает скрипты инициализации `SysV`, как описано в спецификации `Linux Standard Base (LSB)`, что упрощает переход на `systemd`.

По способу использования сервисные юниты `.service` напоминают скрипты инициализации. Для просмотра, старта, остановки, перезагрузки, включения или выключения системных сервисов используется команда `systemctl`. Команды `service` и `chkconfig` по-прежнему включены в систему, но только по соображениям совместимости.

При использовании `systemctl` указывать расширение файла не обязательно. Основные команды `systemctl` описаны в таблице.

Команда	Описание
<code>systemctl start name.service</code>	запуск сервиса;
<code>systemctl stop name.service</code>	остановка сервиса;
<code>systemctl restart name.service</code>	перезапуск сервиса;
<code>systemctl try-restart name.service</code>	перезапуск сервиса только, если он запущен;

Команда	Описание
<code>systemctl reload name.service</code>	перезагрузка конфигурации сервиса;
<code>systemctl status name.service</code>	проверка, запущен ли сервис с детальным выводом состояния сервиса;
<code>systemctl is-active name.service</code>	проверка, запущен ли сервис с простым ответом: active или inactive;
<code>systemctl list-units --type service --all</code>	отображение статуса всех сервисов;
<code>systemctl enable name.service</code>	активирует сервис (позволяет стартовать во время запуска системы);
<code>systemctl disable name.service</code>	деактивирует сервис;
<code>systemctl reenable name.service</code>	деактивирует сервис и сразу активирует его;
<code>systemctl is-enabled name.service</code>	проверяет, активирован ли сервис;
<code>systemctl list-unit-files --type service</code>	отображает все сервисы и проверяет, какие из них активированы;
<code>systemctl mask name.service</code>	заменяет файл сервиса симлинком на <code>/dev/null</code> , делая юнит недоступным для <code>systemd</code> ;
<code>systemctl unmask name.service</code>	возвращает файл сервиса, делая юнит доступным для <code>systemd</code> .

Файлы целей `systemd.target` предназначены для группировки вместе других юнитов `systemd` через цепочку зависимостей. Например юнит `graphical.target`, использующийся для старта графической сессии, запускает системные сервисы GNOME Display Manager (`gdm.service`) и Accounts Service (`accounts-daemon.service`) и активирует `multi-user.target`. В свою очередь `multi-user.target` запускает другие системные сервисы, такие как Network Manager (`NetworkManager.service`) или D-Bus (`dbus.service`) и активирует другие целевые юниты `basic.target`.

В РЕД ОС присутствуют предопределённые цели, похожие на стандартный набор уровней запуска. По соображениям совместимости они также имеют псевдонимы на эти цели, которые напрямую отображаются в уровнях запуска SysV.

- `poweroff.target` (`runlevel0.target`) – завершение работы и отключение системы;
- `rescue.target` (`runlevel1.target`) – настройка оболочки восстановления;
- `multi-user.target` (`runlevel2.target`, `runlevel3.target`, `runlevel4.target`) – настройка неграфической многопользовательской системы;
- `graphical.target` (`runlevel5.target`) – настройка графической многопользовательской системы;
- `reboot.target` (`runlevel6.target`) – выключение и перезагрузка системы.

Команды `runlevel` и `telinit` по-прежнему доступны, но оставлены в системе по соображениям совместимости. Рекомендуется использовать `systemctl` для изменения или настройки системных целей.

Для определения, какой целевой юнит используется по умолчанию, полезна следующая команда:

```
systemctl get-default
```

Для просмотра всех загруженных целевых юнитов воспользуйтесь командой:

```
systemctl list-units --type target
```

а для просмотра вообще всех целевых юнитов командой:

```
systemctl list-units --type target --all
```

Для изменения цели по умолчанию поможет команда:

```
systemctl set-default name.target
```

Для изменения текущей цели:

```
systemctl isolate name.target
```

Команда запустит целевой юнит и все его зависимости и немедленно остановит все остальные.

В РЕД ОС `systemctl` заменяет значительное количество команд управления питанием. Прежние команды сохранены для совместимости, но рекомендуется использовать `systemctl`:

```
systemctl halt – останавливает систему;  
systemctl poweroff – выключает систему;  
systemctl reboot – перезагружает систему.
```

`Systemd` позволяет управлять удалённой машиной по SSH. Для управления используйте команду:

```
systemctl --host <user_name>@<host_name> <command>
```

где `<user_name>` – имя пользователя, `<host_name>` – имя хоста, которым осуществляется удалённое управление, а `<command>` – выполняемая команда `systemd`.

Подробная информация о всех параметрах файла `.service` есть в соответствующем разделе документации по `systemd`.

```
[Unit]  
Description=Daemon to detect crashing apps  
After=syslog.target
```

```
[Service]
ExecStart=/usr/sbin/abrttd
Type=forking
[Install]
WantedBy=multi-user.target
```

Давайте посмотрим на секцию [Unit]. Она содержит общую информацию о сервисе. Такая секция есть не только в сервис-юнитах, но и в других юнитах (например при управлении устройствами, точками монтирования и т.д.). В примере мы даем описание сервиса и указываем на то, что демон должен быть запущен после Syslog.

В следующей секции [Service] непосредственно содержится информация о нашем сервисе. Используемый параметр ExecStart указывает на исполняемый файл нашего сервиса. В Type мы указываем, как сервис уведомляет systemd об окончании запуска.

Финальная секция [Install] содержит информацию о цели, в которой сервис должен стартовать. В данном случае мы говорим, что сервис должен быть запущен, когда будет активирована цель multi-user.target.

Это минимальный работающий файл сервиса systemd. Написав свой, для тестирования скопируйте его в /etc/systemd/system/<имя\_сервиса>.service. Выполните команду:

```
systemctl daemon-reload
```

Systemd узнает о сервисе и вы сможете его запустить.

## 6.6 SELinux

SELinux (Security-Enhanced Linux) обеспечивает усиление защиты путём внесения изменений как на уровне ядра, так и на уровне пространства пользователя. Далее описываются основные принципы, на которых построена работа используемых библиотек SELinux, а также их реализация в РЕД ОС.

### 6.6.1 Введение

В большинстве операционных систем имеются средства управления доступом, которые определяют, может ли определённый объект (пользователь или программа) получить доступ к определённому ресурсу. В РЕД ОС применяется разграничительный контроль доступа (discretionary access control, DAC). Этот метод позволяет ограничить доступ к объектам на основе групп, к которым они принадлежат. Например, для каждого файла определены владелец, группа, а также указаны права доступа к этому файлу. Правами доступа определяется, кто может получить доступ к файлу, кто может открыть его для чтения, кто может внести в него изменения, кто может запустить этот файл на выполнение. Права доступа определены для трёх категорий: пользователь (владелец файла), группа (все пользователи, которые являются членами группы) и другие (все пользователи, которые не являются ни владельцем файла, ни членами группы).

Другим методом управления доступом является управление доступом на основе ролей (role-based access control, RBAC). При использовании RBAC права доступа предоставляются на основе ролей, выдаваемых системой безопасности. Отличие концепции ролей от традиционных групп состоит в том, что группа представляет одного или нескольких пользователей, в то время как роль, хотя она также может быть применена к нескольким пользователям, представляет совокупность полномочий на выполнение определенных действий.

Используемые библиотеки SELinux добавляют в операционную систему поддержку RBAC.

### 6.6.2 Установка

Для установки SELinux требуется установить пакет `selinux-policy`. Это можно сделать, например, воспользовавшись командной строкой с привилегиями `root` пользователя:

```
dnf install selinux-policy
```

После перезагрузки SELinux проиндексирует содержимое жёсткого диска, это может занять некоторое время.

Для настройки SELinux можно использовать различные текстовые редакторы, чтобы настроить вручную его файл конфигурации `/etc/selinux/config`.

### 6.6.3 Утилиты

#### Утилита `audit2allow`

Утилита `audit2allow` создает разрешающие правила политики SELinux из файлов журналов, содержащих сообщения о запрете операций.

Эта утилита сканирует журналы в поиске сообщений, появляющихся, когда система не дает разрешения на операцию. Далее утилита генерирует ряд правил, которые, будучи загруженными в политику, могли бы разрешить эти операции. Однако, данная утилита генерирует только разрешающие правила Type Enforcement (TE). Некоторые отказы в использовании разрешений могут потребовать других изменений политики. Например, добавление атрибута в определение типа, для разрешения существующего ограничения (`constraint`), добавления разрешающего правила для роли или модификации ограничения (`constraint`). В случае сомнений для диагностики можно попробовать использовать утилиту `audit2why`.

Следует с осторожностью работать с выводом данной утилиты, убедившись, что разрешаемые операции не представляют угрозы безопасности. Обычно бывает лучше определить новый домен и/или тип или произвести другие структурные изменения. Лучше избирательно разрешить оптимальный набор операций вместо того, чтобы вслепую применить иногда слишком широкие разрешения, рекомендованные этой утилитой. Некоторые запреты на использование разрешений бывают не принципиальны для приложения. В таких случаях вместо использования разрешительного правила («allow» rule) лучше просто подавить журналирование этих запретов при помощи правила «dontaudit».

Синтаксис:

```
audit2allow [options]
```

Основные опции утилиты `audit2allow` представлены в таблице.

Опция	Значение опции
<code>-a   --all</code>	Прочитать входную информацию из журналов «message» и «audit». Не используется вместе с опцией «-i».
<code>-d   --dmesg</code>	Прочитать входную информацию из вывода команды <code>/bin/dmesg</code> . Обратите внимание, что когда работает <code>auditd</code> , не все сообщения аудита доступны через <code>dmesg</code> . Вместо этого используйте « <code>ausearch -m avc   audit2allow</code> » или «-a».
<code>-f   --fcfile</code> <File Context File>	Добавить файл контекстов в генерируемый пакет модуля. Требуется опция <code>-M</code> .
<code>-h   --help</code>	Вывести краткую справку по использованию.
<code>-i &lt;inputfile&gt;  </code> <code>--input</code> <inputfile>	Прочитать входную информацию из <inputfile>.
<code>-l  </code> <code>--lastreload</code>	Прочитать только часть входной информации, начиная с момента последней перезагрузки политики.
<code>-m</code> <modulename>   <code>--module</code> <modulename>	Генерировать модуль. Требуется вывод <modulename>.
<code>-M &lt;modulename&gt;</code>	Генерировать загружаемый пакет модуля. Опция конфликтует с «-o».
<code>-o</code> <outputfile>   <code>--output</code> <outputfile>	Дописать вывод в <outputfile>.
<code>-r   --requires</code>	Генерировать вывод в синтаксисе загружаемого модуля.
<code>-R   --reference</code>	Генерировать эталонную политику (reference policy), используя установленные макросы. Требуется пакет <code>selinux-policy-devel</code> .
<code>-t   --tefile</code>	Указывает, что выходной файл является te-файлом (type enforcement). Может использоваться для конвертации старого формата политик в новый формат.
<code>-v   --verbose</code>	Включить подробный вывод.

Пример:

Этот пример подходит для системы, использующей пакет `audit`. Если вы не

используете пакет `audit`, сообщения AVC будут появляться в `/var/log/messages`. В этом случае замените `/var/log/audit/audit.log`, используемый в примере, на `/var/log/messages`.

Использование `audit2allow` для генерации монолитной (не модульной) политики:

```
cd /etc/selinux/$ SELINUXTYPE/src/policy
cat /var/log/audit/audit.log | audit2allow >> domains/misc/
local.te
cat domains/misc/local.te
```

```
allow cupsd_config_t unconfined_t:fifo_file { getattr ioctl }
```

Просмотрите `domains/misc/local.te` и измените его:

```
make load
```

Использование `audit2allow` для генерации модульной политики:

```
cat /var/log/audit/audit.log | audit2allow -m local > local.te
cat local.te
```

```
module local 1.0;
require {
    role system_r;
    class fifo_file { getattr ioctl }; type cupsd_config_t; type
unconfined_t;};
allow cupsd_config_t unconfined_t:fifo_file { getattr ioctl };
```

Просмотрите `local.te` и измените его.

Создание модуля политики вручную:

- Скомпилируйте модуль:

```
checkmodule -M -m -o local.mod local.te
```

- Создайте пакет:

```
semodule_package -o local.pp -m local.mod
```

- Загрузите модуль в ядро:

```
semodule -i local.pp
```

- Использование `audit2allow` для генерации и создания модуля политики:

```
cat /var/log/audit/audit.log | audit2allow -M local
```

Создаётся новый type enforcement файл: `local.te`.

- Компиляция политики:

```
checkmodule -M -m -o local.mod local.te
```

- Создание пакета:

```
semodule_package -o local.pp -m local.mod
```

Для того чтобы загрузить только что созданный пакет политики в ядро, вам необходимо выполнить команду:

```
semodule -i local.pp
```

### Утилита secon

Утилита secon — позволяет просмотреть контекст SELinux для файла, программы или ввода пользователя.

Просматривает часть контекста. Контекст берется из файла, идентификатора процесса, ввода пользователя или контекста, в котором была запущена утилита secon.

Синтаксис:

```
secon [-hVurtscmPRfLp] [CONTEXT] [--file] <FILE> [--link] <FILE>
      [--pid] <PID>
```

Основные опции утилиты secon приведены в таблице.

Опция	Значение опции
<code>-V, --version</code>	Посмотреть текущую версию secon.
<code>-h, --help</code>	Вывести информацию по использованию secon.
<code>-P, --prompt</code>	Вывести данные в формате, подходящем для подсказки.
<code>-u, --user</code>	Показать пользователя контекста безопасности.
<code>-r, --role</code>	Показать роль контекста безопасности.
<code>-t, --type</code>	Показать тип контекста безопасности.
<code>-s, --sensitivity</code>	Показать уровень чувствительности (sensitivity level) контекста безопасности.
<code>-c, --clearance</code>	Показать уровень допуска (clearance level) контекста безопасности.
<code>-m, --mls-range</code>	Показать для контекста безопасности в виде диапазона уровень чувствительности (sensitivity level) и уровень допуска (clearance).
<code>-R, --raw</code>	Вывести уровень чувствительности (sensitivity level) и уровень допуска (clearance) в формате без трансляции.
<code>-f, --file</code>	Получить контекст заданного файла <FILE>.
<code>-L, --link</code>	Получить контекст заданного файла <FILE> (не следовать по символическим ссылкам).

Опция	Значение опции
<code>-p, --pid</code>	Получить контекст заданного процесса по идентификатору <code>&lt;PID&gt;</code> .
<code>--pid-exec</code>	Получить <code>exec</code> контекст заданного процесса по идентификатору <code>&lt;PID&gt;</code> .
<code>--pid-fs</code>	Получить <code>fscreate</code> контекст заданного процесса по идентификатору <code>&lt;PID&gt;</code> .
<code>--current, --self</code>	Получить контекст из текущего процесса.
<code>--current-exec, --self-exec</code>	Получить <code>exec</code> контекст из текущего процесса.
<code>--current-fs, --self-fs</code>	Получить <code>fscreate</code> контекст из текущего процесса.
<code>--parent</code>	Получить контекст из родительского процесса текущего процесса.
<code>--parent-exec</code>	Получить <code>exec</code> контекст из родительского процесса текущего процесса.
<code>--parent-fs</code>	Получить <code>fscreate</code> контекст из родительского процесса текущего процесса.

Если не было задано опций, то для того, чтобы `secon` получил контекст из другого источника, может быть задан дополнительный аргумент `CONTEXT`. Если этим аргументом является знак дефиса (`-`), то контекст будет прочитан из стандартного ввода. Если аргументов не было задано, то `secon` будет пытаться прочитать контекст со стандартного ввода, но только в том случае, если стандартный ввод не терминал (`tty`). В этом случае `secon` будет вести себя как будто была передана опция «`--self`».

Если не задана ни одна опция из «`--user`», «`--role`», «`--type`», «`--level`» или «`--mls-range`», то все они будут использованы.

### Утилита `audit2why`

Утилита `audit2why` — позволяет определить из сообщения аудита SELinux причину запрета доступа.

Эта утилита обрабатывает сообщения аудита SELinux, принятые со стандартного ввода, и сообщает, какой компонент политики вызвал каждый из запретов. Если задана опция «`-p`», то используется указанная этой опцией политика, в противном случае используется активная политика. Есть три возможные причины запрета доступа:

- отсутствует или отключено разрешительное TE правило (TE allow rule);
- нарушение ограничения (a constraint violation);
- отсутствует разрешительное правило для роли (role allow rule).

В первом случае разрешительное TE правило может присутствовать в политике, но было отключено через булевы атрибуты. Если же разрешительного правила не было, то оно может быть создано при помощи утилиты `audit2allow`.

Во втором случае могло произойти нарушение ограничения. Просмотрите `policy/constraints` или `policy/mls` для того, чтобы определить искомое ограничение. Обычно проблема может быть решена добавлением атрибута типа к домену.

В третьем случае была произведена попытка сменить роль, при том что не существует разрешительного правила для участвующей при этом пары ролей. Проблема может быть решена добавлением в политику разрешительного правила для этой пары ролей.

Синтаксис:

```
audit2why <options>
```

Основные опции утилиты `audit2why` приведены в таблице.

Опция	Значение опции
<code>--help</code>	Вывести короткую подсказку.
<code>-P</code> <code>&lt;policyfile&gt;</code>	Указать альтернативный файл политики.

Пример:

```
/usr/sbin/audit2why < /var/log/audit/audit.log
type=KERNEL msg=audit(1115316408.926:336418): avc: denied
{ getattr } for path=/home/ sds dev=hda5 ino=1175041
scontext=root:secadm_r: secadm_t:s0-s9:c0.c127
tcontext=user_u:object_r:user_home_dir_t:s0 tclass=dir
```

Причиной является: Отсутствие или отключение разрешительного TE правила. Разрешительное TE правило может присутствовать в политике, но было отключено через булевы переключатели; проверьте булевы переключатели. Вы можете посмотреть необходимые разрешительные правила, запустив `audit2allow` и подав это сообщение аудита на ввод.

```
type=KERNEL msg=audit(1115320071.648:606858): avc: denied
{ append } for name=.bash_history dev=hda5 ino=1175047
scontext=user_u:user_r:user_t:s1-s9:c0.c127 tcontext=user_u:
object_r:user_home_t:s0 tclass=file
```

Причиной является: Нарушение ограничения. Проверьте `policy/constraints`. Обычно, для разрешения ограничения необходимо добавить в домен атрибут типа.

### Утилита `chcat`

Утилита `chcat` — позволяет изменить категорию безопасности SELinux для файла.

Изменить/Удалить категорию безопасности для каждого файла или пользователя. Используйте +/- для добавления/удаления категории у файла или пользователя.

**Примечание.** При удалении категории вы должны задать «--» в командной строке до использования синтаксиса «-Category». Это сообщит команде, что вы закончили вводить опции и теперь задаёте имя категории.

Синтаксис:

```
chcat category <file...>
chcat -l category <user...>
chcat [[+|-]category...] <file...>
chcat -l [[+|-]category...] <user...>
chcat [-d] <file...>
chcat -l [-d] <user...>
chcat -L [ -l ] [ <user ...> ]
```

Основные опции утилиты chcat приведены в таблице.

Опция	Значение опции
-d	Удалить категорию из каждого ФАЙЛА/ПОЛЬЗОВАТЕЛЯ.
-L	Вывести доступные категории.
-l	Сообщить команде chcat, что нужно работать с пользователями вместо файлов.

При работе с файлами данный скрипт вызывает команду chcon.

### Утилита fixfiles

Утилита fixfiles — позволяет восстановить контекст безопасности SELinux для файла.

Синтаксис:

```
fixfiles [-F] [ -R rpmpackagename[,rpmpackagename...] ]
[ -C PREVIOUS_FILECONTEXT ] [-l logfile ] [-o outputfile ] {check
| restore | [-F] relabel | verify }" fixfiles [-F] [-l logfile ]
[-o outputfile ]{ check | restore|[-f] relabel | verify }
[[dir/file] ... ]
```

Утилита fixfiles используется, в первую очередь, когда необходимо скорректировать базу данных с контекстами безопасности (расширенные атрибуты) для файловой системы.

Его также можно запускать в любое время для добавления поддержки новой политики или чтобы убедиться в том, что файлам присвоены нужные контексты. По умолчанию скрипт обновляет метки на всех смонтированных файловых системах ext2, ext3, xfs и jfs, даже если они не имеют опции монтирования с контекстом безопасности. Вы можете использовать флаг «-R» для того, чтобы в качестве альтернативы использовать rpm-пакет.

Основные опции, используемые утилитой `fixfiles`, представлены в таблице.

Опция	Значение опции
<code>-l logfile</code>	Сохранить вывод в заданном файле <code>logfile</code> .
<code>-o outputfile</code>	Сохранить все имена файлов, имеющих <code>&lt;file_context&gt;</code> , отличающийся от контекста по умолчанию в файл <code>outputfile</code> .
<code>-F</code>	Принудительно установить контекст как в <code>&lt;file_context&gt;</code> для настраиваемых файлов ( <code>customizable files</code> ).
<code>-f</code>	Не предупреждать об удалении из директории <code>/tmp</code> .
<code>-R rpm_package_name [,rpm_package_name..</code>	При помощи базы данных <code>rpm</code> , найти все файлы из заданного пакета и восстановить для них контекст ( <code>-a</code> выдаст все файлы из базы данных <code>RPM</code> ).
<code>-C PREVIOUS_FILECONTEXT</code>	Запустить <code>diff</code> для сравнения файла <code>PREVIOUS_FILECONTEXT</code> с текущим и восстановить контекст на всех затронутых файлах.

Аргументы утилиты `fixfiles` описаны в таблице.

Аргумент	Значение аргумента
<code>check</code>	Вывести все некорректные метки контекста файлов. Показать и старый и новый контекст, но не изменять его.
<code>restore</code>	Изменить все некорректные метки контекста файлов.
<code>relabel</code>	Задать вопрос об удалении содержимого директории <code>/tmp</code> и, затем, изменения некорректных меток контекста файлов для приведения в соответствие с файлом <code>&lt;file_contexts&gt;</code> .
<code>verify</code>	Вывести все файлы с некорректным контекстом, не менять его.
<code>&lt;dir/file&gt;...</code>	Список файлов или директорий, для которых вы хотите проверить контекст.

### Утилита `genhomedircon`

Утилита `genhomedircon` — позволяет создать спецификации с контекстом SELinux для файлов домашних директорий пользователей.

Синтаксис:

```
genhomedircon [ -d selinuxdir ] [-n | --nopasswd] [-t selinuxtype] [-h]
```

Основные опции утилиты `genhomedircon` представлены в таблице.

Опция	Значение опции
-h	Вывести короткую подсказку.
-d selinuxdir (--directory)	Директория, где установлены файлы selinux. По умолчанию /etc/selinux.
-n --nopasswd	Указать утилите не брать информацию о домашних директориях из базы паролей.
-t selinuxtype (--type)	Указать тип установки selinux. По умолчанию - «целевая» («targeted»).

Данная утилита используется для генерации спецификации с контекстом SELinux для файлов домашних директорий пользователей, основываясь на их записи prefix в записи пользователя semanage. genhomedircon запускается во время создания политики. Утилита также может запускаться автоматически каждый раз, когда утилита semanage изменяет запись user или login. А именно, мы заменяем макросы HOME\_ROOT, HOME\_DIR и ROLE в файле /etc/selinux/«SELINUXTYPE»/contexts/files/homedir\_template на специфичные для пользователя сгенерированные значения.

HOME\_ROOT и HOME\_DIR заменяются на месторасположения пользовательских домашних директорий. По умолчанию - /home.

ROLE заменяется на значение, основанное на записи prefix в записи. user genhomedircon ищет все строчки для простых (не системных) пользователей в базе данных паролей. Такими пользователями будут те, чей UID больше или равен STARTING\_UID (по умолчанию - 500), и для кого в поле login shell не стоит «/sbin/nologin» или «/bin/false».

### Утилита load\_policy

Утилита load\_policy — позволяет загрузить новую политику SELinux в ядро. Синтаксис:

```
load_policy [-bq]
```

load\_policy - утилита, используемая для загрузки/замены политики в ядре. По умолчанию при загрузке политики load\_policy сохраняет текущие значения переключателей.

Основные опции утилиты load\_policy приведены в таблице.

Опция	Значение опции
-b	Сбросить переключатели в значения, определённые в политике.
-q	Скрыть предупреждения.

### Утилита open\_init\_pty

Утилита open\_init\_pty – указывает запустить программу в псевдо-терминале. Используется run\_init для того, чтобы запустить программу после установки

правильного контекста. Эта программа берет новый псевдо-терминал, порождает (forks) процесс-наследник, который привязывается к новому псевдо-терминалу. Затем он подключает физический терминал, с которого он был вызван, к псевдо-терминалу, передавая ввод с клавиатуры процессу-наследнику и отправляя вывод процесса-наследника на физический терминал.

Он устанавливает атрибуты псевдо-терминала, основываясь на атрибутах физического терминала, а затем устанавливает пользовательский терминал в RAW-режим, не забыв сбросить его при выходе.

Синтаксис:

```
open_init_pty SCRIPT [[ARGS]...]
```

### Утилита restorecon

Утилита restorecon - позволяет восстановить заданный по умолчанию контекст безопасности SELinux для файла (файлов).

Эта программа используется, в первую очередь, когда необходимо установить контекст безопасности (расширенные атрибуты) для одного или более файлов.

Ее можно запускать в любое время для коррекции ошибок, для добавления поддержки новой политики или с опцией «-n», чтобы убедиться в том, какой контекст присвоен файлу.

Синтаксис:

```
restorecon [-o outfile] [-R] [-n] [-v] [-e directory ]
pathname... restorecon -f infile [-o outfile]
[-e directory ] [-R] [-n] [-v] [-F]
```

Основные опции утилиты restorecon приведены в таблице.

Опция	Значение опции
-i	Игнорировать несуществующие файлы.
-f <infile>	<infile> содержит список файлов, которые будут обработаны. Для того чтобы использовать стандартный ввод, используйте «-» (символ дефис).
-e <directory>	Задать директорию, которую нужно исключить из обработки (для нескольких директорий повторите опцию).
-R -r	Рекурсивно поменять метки для файлов и директорий.
-n	Не менять метки файлов.
-o <outfile>	Сохранить список файлов с некорректным контекстом в <outfile>.
-v	Показать изменения меток файлов.
-vv	Показать изменения меток файлов, если изменился тип, роль или пользователь.

Опция	Значение опции
-F	Если произошли изменения, то принудительно установить контекст как в <file_context> для настраиваемых файлов (customizable files) или секции пользователя.

Ниже описаны аргументы, используемые утилитой restorecon.

Аргумент	Значение аргумента
pathname...	Путь к файлу(файлам), требующим изменения меток.
restorecon	Не обрабатывает файлы и директории по символическим ссылкам на них.

### Утилита restorecond

Утилита restorecond - служба, который отслеживает создание файлов, и выставляет для них заданный по умолчанию контекст SELinux.

Данное руководство описывает программу restorecond. Используя inotify, данный демон следит за файлами, перечисленными в /etc/selinux/restorecond.conf. Демон позволяет убедиться, что эти файлы при создании будут иметь правильный контекст, который определен в политике.

Синтаксис:

```
restorecond [-d]
```

Опции утилиты restorecond описаны в таблице.

Опция	Значение опции
-d	Включить режим отладки. Приложение все так же исполняется на переднем плане, но начинает выводиться большое число отладочных сообщений.

### Утилита run\_init

Утилита run\_init - запускает скрипт init в правильном контексте, который определен в /etc/selinux/targeted/contexts/initrc\_context.

Синтаксис:

```
run_init SCRIPT [[ARGS]...]
```

Основные файлы, используемые утилитой run\_init, описаны в таблице.

Файл	Описание файла
/etc/passwd	Информация об учетных записях пользователей.
/etc/shadow	Зашифрованные пароли и информация об устаревании паролей.

Файл	Описание файла
/etc/selinux/ targeted/ contexts/ initrc_context	Содержит контекст, в котором должны исполняться инициализационные скрипты.

### Утилита semanage

Утилита `semanage` - утилита управления политикой SELinux.

Утилита `semanage` используется для настройки некоторых элементов политики SELinux без необходимости модификации или повторной компиляции исходного текста политики. В число таких настроек входит сопоставление имён пользователей ОС пользователям SELinux (которые контролируют исходный контекст безопасности, присваиваемый пользователям ОС во время их регистрации в системе, и ограничивают доступный набор ролей).

Также в число настраиваемых элементов входит сопоставление контекстов безопасности для различных видов объектов, таких как: сетевые порты, интерфейсы, сетевые узлы (хосты), а также контексты файлов.

Обратите внимание, что при вызове команды «`semanage login`» сопоставляются имена пользователей ОС (logins) пользователям SELinux. А при вызове команды «`semanage user`» сопоставляются пользователи SELinux доступному набору ролей. В большинстве случаев администратором выполняется настройка только первого типа сопоставлений. Второй тип сопоставлений, как правило, определяется базовой политикой и обычно не требует модификации.

Синтаксис:

```
semanage {login|user|port|interface|fcontext|translation} -l [-n]
semanage login -{a|d|m} [-sr] <login_name>
semanage user -{a|d|m} [-LrRP] <selinux_name>
semanage port -{a|d|m} [-tr] [-p protocol] <port> | <port_range>
semanage interface -{a|d|m} [-tr] <interface_spec>
semanage fcontext -{a|d|m} [-fst] <file_spec>
semanage translation -{a|d|m} [-T] <level>
```

Основные опции, используемые утилитой `semanage`, описаны в таблице.

Опция	Значение опции
-a, --add	Добавить запись ОБЪЕКТА с заданным ИМЕНЕМ.
-d, --delete	Удалить запись ОБЪЕКТА с заданным ИМЕНЕМ.
-f, --ftype	Тип файла. Эта опция используется совместно с « <code>fcontext</code> ». Тип необходимо указывать в таком же виде, как и в выводе программы <code>ls</code> , иными словами, « <code>--</code> » указывает на обыкновенные файлы, а « <code>-d</code> » – только на директории.
-h, --help	Показать справку.
-l, --list	Вывести список ОБЪЕКТОВ.

Опция	Значение опции
-L, --level	Уровень чувствительности SELinux, s0 по умолчанию (только для систем с поддержкой MLS/MCS).
-m, --modify	Изменить ОБЪЕКТ с заданным ИМЕНЕМ записи.
-n, --noheading	Не выводить шапку таблицы при печати списка ОБЪЕКТОВ.
-p, --proto	Протокол, используемый для указанного порта (tcp udp).
-r, --range	Диапазон безопасности MLS/MCS (только для систем с поддержкой MLS/MCS).
-R, --role	Роли SELinux. При указании нескольких ролей нужно отделить их пробелами и заключить в кавычки или указывать опцию «-R» необходимое число раз.
-P, --prefix	Префикс SELinux. При установке меток на домашние директории пользователей префикс добавляется к <home_dir_t> и <home_t>.
-s, --seuser	Имя пользователя SELinux.
-t, --type	Тип объекта SELinux.
-T, --trans	Трансляция SELinux (SELinux Translation).

Примеры:

Просмотреть сопоставления для пользователей SELinux:

```
semanage user -l
```

Разрешить joe регистрироваться как staff\_u:

```
semanage login -a -s staff_u joe
```

Определить контекст файлов для всего, расположенного в /web (потом это определение используется утилитой restorecon):

```
semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
```

Разрешить демону Apache прослушивать порт с номером 81:

```
semanage port -a -t http_port_t -p tcp 81
```

### Утилита semodule

Утилита semodule - утилита, используемая для управления пакетами модулей политики SELinux. Управление включает в себя задачи установки, обновления, просмотра и удаления пакетов модулей. semodule можно также использовать

для принудительного пересоздания политики из хранилища модулей и/или для принудительной перезагрузки политики без выполнения каких-либо других операций. `semodule` работает с пакетами модулей, созданными утилитой `semodule_package`. По соглашению такие файлы имеют расширение `.pp` (policy package). Однако присваивать именно такое расширение не обязательно.

Синтаксис:

```
semodule [options]... MODE [MODES]...
```

Основные опции утилиты `semodule` описаны в таблице.

Опция	Значение опции
<code>-R, --reload</code>	Принудительно перезагрузить политику.
<code>-B, --build</code>	Принудительно пересоздать политику (если не используется опция <code>-n</code> , то происходит и ее перезагрузка).
<code>-i, --install=MODULE_PKG</code>	Установить/заменить модуль пакета.
<code>-u, --upgrade=MODULE_PKG</code>	Обновить существующий модуль пакета.
<code>-b, --base=MODULE_PKG</code>	Установить/заменить базовый модуль пакета.
<code>-r, --remove=MODULE_NAME</code>	Удалить существующий модуль.
<code>-l, --list-modules</code>	Показать список установленных модулей (кроме базовых).
<code>-s, --store</code>	Имя хранилища, с которым производятся операции.
<code>-n, --noreload</code>	Не перезагружать политику после выполнения операции.
<code>-h, --help</code>	Вывести подсказку.
<code>-v, --verbose</code>	Подробный вывод.

Примеры:

Установить или заменить базовый пакет политики:

```
semodule -b base.pp
```

Установить или заменить не базовый пакет политики:

```
semodule -i httpd.pp
```

Показать список установленных модулей (кроме базовых):

```
semodule -l
```

Установить или заменить все не базовые пакеты в текущей директории:

```
semodule -i *.pp
```

Установить или заменить все модули в текущей директории:

```
ls *.pp | grep -Ev "base.pp|enableaudit.pp" | xargs
/usr/sbin/semodule -b base.pp -
```

### Утилита `semodule_deps`

Утилита `semodule_deps` - показать зависимости между пакетами модулей политики SELinux.

Для каждого модуля она выводит список необходимых для удовлетворения зависимостей модулей. Утилита имеет дело только с абсолютно необходимыми, а не опциональными зависимостями.

Для того чтобы получить от `semodule_deps` действительно полезную информацию, необходимо, чтобы передаваемые ей пакеты не имели не удовлетворённых зависимостей. На практике это означает, что, как правило, список модулей будет весьма длинным.

По умолчанию, базовые модули исключаются, поскольку почти каждый модуль зависит от базовых. Опция «-b» позволяет включить и эти зависимости.

В дополнение к выводу, форматированному для удобного восприятия человеком, `semodule_deps` с опцией «-g» умеет выгружать данные в формате Graphviz (<http://www.graphviz.org/>). Это удобно для создания графического представления зависимостей.

Синтаксис:

```
semodule_deps [-v -g -b] basemodpkg modpkg1 [modpkg2 ... ]
```

Основные опции утилиты `semodule_deps` приведены в таблице.

Опция	Значение опции
-v	Подробный вывод.
-g	Вывод информации о зависимостях в формате Graphviz.
-b	Включить в вывод зависимостей базовые модули (по умолчанию не используется).

### Утилита `semodule_expand`

Утилита `semodule_expand` - утилита добавления пакета модуля политики SELinux.

Данная утилита не входит в число утилит, необходимых при ежедневной работе с SELinux.

Обычно такие операции, как добавление (expanding) выполняются незаметно для пользователя при помощи libsemanage в ответ на команды semodule.

Базовые пакеты модулей политики могут создаваться утилитой semodule\_package или semodule\_link (когда в единый пакет связываются несколько пакетов).

Синтаксис:

```
semodule_expand [-V -c <version>] basemodpkg <outputfile>
```

Основные опции утилиты semodule\_expand приведены в таблице.

Опция	Значение опции
-V	Отобразить версию.
-c <version>	Версия создаваемой политики.

### Утилита semodule\_link

Утилита semodule\_link - утилита объединения нескольких пакетов модулей политики SELinux.

Данная утилита не входит в число утилит, необходимых при каждодневной работе с SELinux. Обычно, такие операции как связывание выполняются незаметно для пользователя при помощи «libsemanage» в ответ на команды semodule. Пакеты модулей создаются утилитой semodule\_package.

Синтаксис:

```
semodule_link [-Vv] [-o <outfile>] basemodpkg <modpkg1>  
[<modpkg2>]...
```

Основные опции утилиты semodule\_link приведены в таблице.

Опция	Значение опции
-V	Отобразить версию.
-v	Подробный вывод.
-o <output file>	Объединённый пакет модулей политики, созданный утилитой.

### Утилита semodule\_package

Утилита semodule\_package - это утилита, используемая для создания пакета модуля политики SELinux из бинарного модуля политики и других источников данных, таких как файл контекстов. semodule\_package создает пакеты из бинарных модулей политики, созданных, в свою очередь, при помощи «checkmodule». Пакеты политик, созданные semodule\_package, могут быть установлены утилитой semodule.

Синтаксис:

```
semodule_package -o <output file> -m <module> [-f <file contexts>]
```

Примеры:

Создать пакет модуля политики для базового модуля.

```
semodule_package -o base.pp -m base.mod -f file_contexts
```

Создать пакет модуля политики для модуля httpd.

```
semodule_package -o httpd.pp -m httpd.mod -f httpd.fc
```

Создать пакет модуля политики для локальных TE-правил (TE rules) без использования файла контекстов.

```
semodule_package -o local.pp -m local.mod
```

Основные опции утилиты `semodule_package` приведены в таблице.

Опция	Значение опции
<code>-o --outfile &lt;output_file&gt;</code>	Пакет модуля политики, создаваемый данной утилитой.
<code>-s --seuser &lt;seuser_file&gt;</code>	Файл <code>seuser</code> будет включён в пакет.
<code>-u --user_extra &lt;user_extra_file&gt;</code>	Файл <code>&lt;user_extra&gt;</code> будет включён в пакет.
<code>-m --module &lt;module file&gt;</code>	Файл модуля политик будет включён в пакет.
<code>-f --fc &lt;file context file&gt;</code>	Файл с контекстами файлов для модуля (опционально).
<code>n --nc &lt;netfilter_context_file&gt;</code>	Включить в пакет файл контекста <code>netfilter</code> .

### Утилита `sestatus`

Утилита `sestatus` - позволяет просмотреть состояние SELinux.

Эта утилита предназначена для просмотра статуса системы, использующей SELinux. Она показывает информацию о том, включён ли SELinux в целом, загруженную политику, а также в каком режиме система - режиме блокировок (`enforcing mode`) или режиме предупреждений (`permissive mode`). Утилита также может применяться для просмотра контекста безопасности файлов и процессов, описанных в файле `/etc/sestatus.conf`.

Пример запуска:

```
sestatus
```

```
SELinux status: enabled SELinuxfs mount: /selinux Current Mode:
permissive Policy version: 16
```

Синтаксис:

```
sestatus [-v] [-b]
```

Основные опции утилиты `sestatus` приведены в таблице.

Опция	Значение опции
<code>-v</code>	Просмотреть контекст безопасности файлов и процессов, описанных в файле <code>/etc/sestatus.conf</code> . Для символической ссылки также будет показан и контекст файла, на который она ссылается.
<code>-b</code>	Посмотреть текущее состояние переключателей.

### Утилита `setfiles`

Утилита `setfiles` - позволяет установить контекст безопасности SELinux для файла.

Эта программа используется, в первую очередь, когда необходимо инициализировать базу данных с контекстами безопасности (расширенные атрибуты) для одной или более файловых систем.

Первоначально программа выполняется как часть процесса установки SELinux. Ее можно запускать в любое время для следующих задач: коррекция ошибок, добавление поддержки новой политики, просто чтобы убедиться в том, какой контекст присвоен файлу (с опцией «-n»).

Синтаксис:

```
setfiles [-c <policy> ] [-d] [-l] [-n] [-e <directory> ]
[-o <filename> ] [-q] [-s] [-v] [-vv] [-W] [-F] <spec_file>
pathname...
```

Основные опции утилиты `setfiles` приведены в таблице.

Опция	Значение опции
<code>-c</code>	проверить соответствие контекста тому, что определён в двоичном файле политики.
<code>-d</code>	показать, какая спецификация соответствует каждому файлу «-l» – отразить изменения меток в syslog.
<code>-n</code>	не менять метки файлов.
<code>-q</code>	подавить вывод, не относящийся к ошибкам.
<code>-r</code> <code>&lt;rootpath&gt;</code>	использовать альтернативный путь к корневой директории.

Опция	Значение опции
-e <directory>	задать директорию, которую нужно исключить из обработки (для нескольких директорий повторите опцию).
-F	Принудительно установить контекст как в <file_context> для настраиваемых файлов (customizable files).
-o <filename>	сохранить список файлов с некорректным контекстом в <filename>.
-s	получить список файлов со стандартного ввода, вместо использования пути, определяемого в командной строке.
-v	показать изменения меток файлов, если изменился тип или роль.
-vv	показать изменения меток файлов, если изменился тип, роль или пользователь.
-W	вывести предупреждения, если встретятся спецификации, которым не соответствует ни один файл.

Основные аргументы утилиты setfiles описаны в таблице.

Аргумент	Значение аргумента
spec_file	<p>Файл со спецификациями, содержащий строки следующего вида: regex [ -type ] ( «context»   «none» ).</p> <p>В начале и в конце строки расположены регулярные выражения. Необязательное поле указывает тип файла в том же виде, как в выводе программы ls, иными словами, «--» указывает только на обыкновенные файлы, а «-d» – только на директории. В поле «context» может быть указан контекст безопасности или строка «none», которая указывает, что контекст файла не изменяется.</p> <p>Приоритет имеют спецификации, указанные последними. Если заданно несколько разных спецификаций с различающимся контекстом безопасности для нескольких жестких ссылок на файл, то, несмотря на выводимые предупреждения, файл получит контекст, указанный в последней из таких спецификаций. Если последняя из таких спецификаций содержит «none», то она не учитывается.</p>
pathname...	<p>Путь к корневой директории для каждой из файловых систем, для которых проставляются контексты. Не используется вместе с опцией «-s».</p>

### Утилита setsebool

Утилита setsebool устанавливает текущее значение для одного переключателя или целого списка переключателей SELinux. В качестве значения можно устанавливать «1», «true» или «on» для включения переключателя. Для выключения

можно использовать «0», «false» или «off».

Если не использовать опцию «-P», то изменения коснутся только текущих значений переключателей. Значения по умолчанию, которые устанавливаются во время загрузки, при этом не меняются.

Если задана опция «-P», то все текущие значения переключателей сохраняются в файле политики на диске. Таким образом, их значение сохранится и после перезагрузки.

Синтаксис:

```
setsebool [ -P ] <boolean> <value> | <bool1=val1> <bool2=val2>...
```

### Утилита sealert

Утилита sealert позволяет в режиме реального времени отображать для текущего пользователя обнаруженные конфликты и возможные нарушения информационной безопасности.

В случае если система обнаружила сбой в области системного трея возникает всплывающее уведомление (рисунок 6.2).

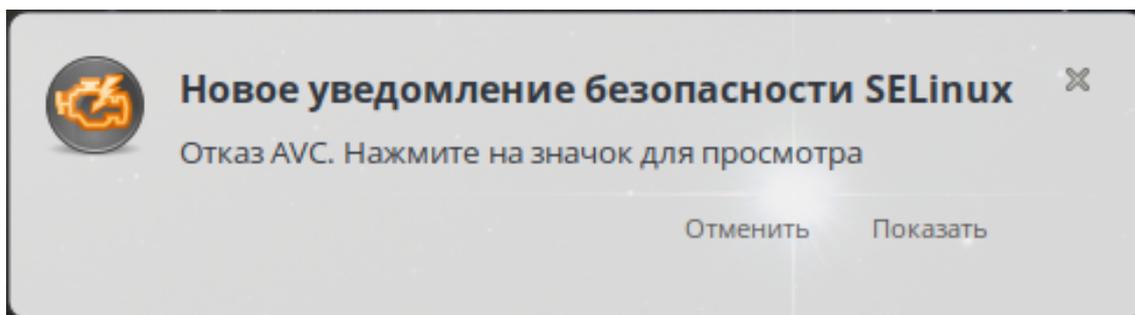


Рисунок 6.2 — Уведомление о нарушении безопасности

По нажатию кнопки «Показать» отображается окно с расширенной информацией о событии (рисунок 6.3).

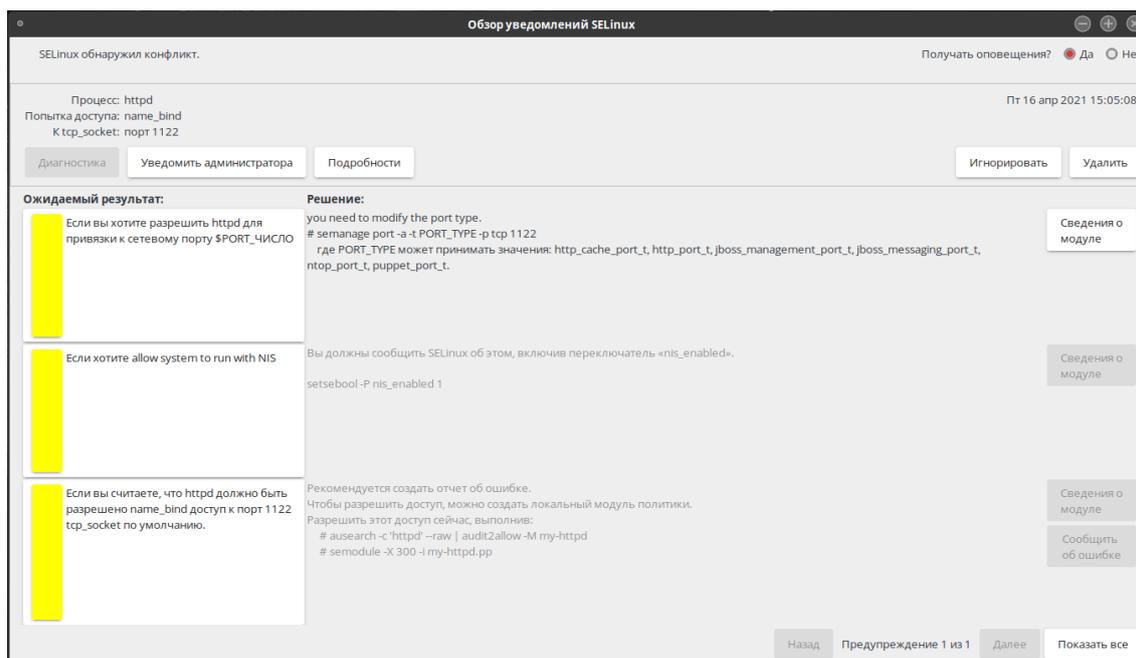


Рисунок 6.3 — Окно уведомлений

Также пользователь может вызвать это окно с консоли командой:

```
sealert
```

Из текущего окна пользователь может просмотреть подробности произошедшего события, уведомить администратора ОС, удалить информацию данного уведомления или игнорировать информацию.

В расширенной информации приводятся сведения об ожидаемом результате и возможные пути решения проблемы.

## 6.7 РАМ

РАМ или Pluggable Authentication Modules (подключаемые модули аутентификации) — это модульный подход к системе аутентификации. Они позволяют сторонним службам предоставлять модуль аутентификации для обеспечения доступа к службе для систем с поддержкой РАМ. Службы, использующие РАМ для аутентификации, могут использовать их сразу же, без необходимости дополнительной пересборки.

На сервере РАМ (Pluggable Authentication Modules) могут использоваться для управления аутентификацией (как часть управления предоставлением доступа). При использовании РАМ сервисам нет необходимости поддерживать собственную систему аутентификации. Вместо этого они полагаются на модули РАМ, доступные в системе.

Любой сервис при необходимости может использовать собственную конфигурацию РАМ, хотя в большинстве случаев аутентификация выполняется одинаково во множестве сервисов. Вызывая модули РАМ, сервисы могут поддерживать двухфакторную аутентификацию «из коробки», сразу же использовать

централизованные хранилища аутентификационных средств и многое другое.

РАМ предоставляют гибкую модульную архитектуру для следующих сервисов:

- управление аутентификацией - проверяет, существует ли пользователь под которым пытаются зайти;
- управление учётными записями - проверяет, что пароль пользователя не истёк или имеет ли пользователь право обращаться к определённому сервису;
- управление сеансами - выполняет определённые задачи во время входа или выхода пользователя из системы (аудит, монтирование файловых систем и так далее);
- управление паролями - предлагает интерфейс для сброса пароля и тому подобное.

При работе с РАМ администраторы очень быстро поймут принципы, по которым функционирует РАМ.

Во-первых, это «независимость от бэк-энда». Приложениям, поддерживающим РАМ, нет необходимости учитывать низкоуровневую логику, чтобы работать с бэк-эндами. Используя РАМ, приложения отделяют логику работы бэк-энда от своей. Всё, что им нужно сделать — это вызвать функцию РАМ.

Другим принципом является «независимость от конфигурации». Администраторам не нужно знать, как настраивать десятки различных приложений, чтобы заставить их поддерживать аутентификацию. Вместо этого им достаточно воспользоваться одной конфигурационной структурой, предоставляемой РАМ.

Последним принципом, являющимся также частью названия РАМ, является «подключаемая архитектура». Когда необходимо интегрировать новый бэк-энд, всё, что нужно сделать администратору — это установить библиотеку для этого бэк-энда (большинство модулей используют один файл настроек). Начиная с этого момента модуль становится доступен для использования приложениями. Администраторы могут настроить аутентификацию для использования этого бэк-энда и просто перезапустить приложение.

Приложения, для которых необходимо использование РАМ, линкуются с библиотекой РАМ (`libram`) и могут вызывать нужные функции работы с указанными выше службами. Кроме этого, в приложении не нужно ничего реализовывать специфичного для работы с этими сервисами, так как эту задачу на себя берёт РАМ. И когда пользователь захочет аутентифицироваться, скажем, в веб-приложении, то это приложение вызывает РАМ (передавая ему идентификатор и, возможно, пароль или запрос) и проверяет возвращаемые данные, чтобы принять решение, аутентифицировался ли пользователь и имеет ли он доступ к приложению. Внутренней задачей РАМ является определение, где необходимо аутентифицировать пользователя.

Сильной стороной РАМ является то, что любой желающий может создать модули РАМ для интеграции с любым поддерживающим РАМ сервисом или приложением. Если какая-нибудь компания выпускает новый сервис для аутентификации, всё, что нужно будет сделать, — это предоставить для взаимодействия с этим сервисом модуль РАМ, после чего любое использующее РАМ приложение сможет незамедлительно работать с этим сервисом: нет необходимости что-то

пересобирать или улучшать.

Другой важной особенностью PAM является то, что они поддерживают объединение в цепочки нескольких модулей. Пример конфигурационного файла PAM для некоего сервиса:

```
# Аутентификация
auth required pam_env.so
auth required pam_ldap.so
# Управление учётными записями
account required pam_ldap.so
# Управление паролями
password required pam_ldap.so
# Управление сеансами
session optional pam_loginuid.so
session required pam_selinux.so close
session required pam_env.so
session required pam_log.so level=audit
session required pam_selinux.so open multiple
session optional pam_mail.so
```

Видно, что конфигурационный файл разделён на четыре области сервисов, которые поддерживают PAM: аутентификация, управление учётными записями, управление паролями и управление сеансами.

Каждый из этих разделов в файле вызывает один или несколько модулей PAM. Например, «pam\_env.so» устанавливает переменные среды, которые могут быть использованы последующими модулями. Код, возвращаемый модулем PAM, вместе с управляющими директивами (в данном примере — «required» или «optional») позволяет PAM решать, что делать дальше.

PAM поддерживают следующие управляющие директивы:

- **required** – указанный модуль PAM должен вернуть код успеха для того, чтобы весь сервис (например, аутентификация) была успешен. Если модуль PAM вернёт код неудачи, остальные модули будут всё равно вызваны (хотя уже точно известно, что сам сервис будет недоступен);
- **requisite** – указанный модуль PAM должен вернуть код успеха для того, чтобы весь сервис был доступен. В отличие от «required», если модуль PAM вернёт код неудачи, директива сразу же завершится, и сам сервис будет недоступен;
- **sufficient** – если указанный модуль PAM вернёт код успеха, весь сервис будет разрешён. Оставшиеся модули PAM не будут проверяться. Однако, если модуль PAM вернёт код неудачи, оставшиеся модули пройдут проверку, а неудача данного модуля не будет приниматься во внимание;
- **optional** – код успеха или неудачи указанного модуля PAM будут иметь значение, если это единственный модуль в стеке.

Цепочки модулей позволяют выполнить множественную аутентификацию, выполнить несколько задач в процессе создания сеанса и тому подобное.

Так как конфигурационные файлы PAM управляют процессом аутентификации в приложении, очень важно правильно с ними взаимодействовать. Файлы

обычно располагаются в каталоге `/etc/pam.d/`.

В больших организациях или в требовательных к безопасности системах любая модификация конфигурационных файлов PAM должна подвергаться соответствующему аудиту.

Это же относится к тому месту, где располагаются модули PAM (`/lib/security` или `/lib64/security`).

Помимо файлов-сценариев для некоторых модулей могут использоваться дополнительные файлы конфигурации. Все они расположены в каталоге `/etc/security` и каждый файл предназначен для конкретной группы настроек.

**time.conf** – здесь вы сможете ограничить время доступа пользователей с различных терминалов к различным сервисам. Например, запретить входить в систему с первой виртуальной консоли администратору во время выходных. Эти настройки обслуживает модуль «`pam_time`» и, соответственно, если вы желаете, чтобы ваши ограничения возымели действие, модуль должен быть прописан в соответствующем сценарии.

**pam\_env.conf** – здесь можно ограничить возможности в изменении отдельных переменных среды пользователями. Работает под руководством модуля «`pam_env`».

**limits.conf** – здесь можно индивидуально или для группы ограничить: размер core-файла, максимальный допустимый размер файла, максимальное количество открытых файлов, запущенных процессов, сколько раз можно одновременно зайти в систему и т.д. Руководящий модуль «`pam_limits`».

**access.conf** – так как PAM имеет средства аутентификации по сети, то подобные настройки являются полезными ибо контролируется не только «кто может зайти» или «не зайти», но и «откуда». Контролируется «`pam_access`».

**group.conf** – можно указать, какой группе будет принадлежать служба, запущенная определенным пользователем, в определённое время с определённого терминала. Контролируется «`pam_time`» и «`pam_group`».

**console.perms** – несколько выбивается своим названием, но не функциями. Здесь определяются права, получаемые привилегированными пользователями к консоли во время входа в систему и возвращаемые при выходе. Модуль «`pam_console`».

Список модулей.

**pam\_cracklib:** Тип «`password`». Проверяет ваш пароль на стойкость, не является ли он, например, палиндромом (примечание – это не обязательно при использовании модуля «`pam_unix`»). Полезен для программ, задающих пароли. Полезные параметры: `retry=N` - даётся N попыток на исправление ошибки, `diffok=N` - должно быть изменено минимум N символов при смене пароля, `minlen=N` - минимальный размер пароля, `dcredit=N` `ucredit=N` `lcredit=N` `ocredit=N` - в пароле должно присутствовать минимум N цифр, строчных, прописных букв и других символов.

**pam\_deny:** Тип любой. Всегда перекрывает доступ.

**pam\_env:** Тип «`auth`». Контролирует сохранность переменных среды. Полезный параметр `conffile=S` - задаёт альтернативное название файла конфигурации.

**pam\_ftp:** Тип «`auth`». Предназначен для организации анонимного доступа. То есть получив имя пользователя «`anonymous`», ждёт в качестве пароля что-то

похожее на его почтовый адрес. Полезные параметры: `ignore` - не обращать внимание похож ли пароль на почтовый адрес, `users=XXX,YYY` - позволяет анонимный вход для пользователей из этого списка.

**pam\_group:** Тип «auth». Предназначение ясно из описания конфигурационного файла «group.conf».

**pam\_lastlog:** Тип «auth». Сообщает о времени и месте входа в систему. Обновляет `/var/log/wtmp` файл. Полезные параметры: «nodate», «noterm», «nohost», «silent» - не выводить в сообщении даты, терминала, машины или вообще ничего, «never» - если пользователь никогда ранее не появлялся, то его приветствуют.

**pam\_limits:** Тип «session». Предназначение указано выше при описании файла «limits.conf». Полезный параметр: `conf=S` - альтернативное имя конфигурационного файла.

**pam\_listfile:** Тип «auth». Предназначен для организации доступа на основе конфигурационных файлов-списков например `/etc/ftpaccess`. Для примера смотрите соответствующие файлы сценариев. Возможные параметры: `onerr=succeed|fail`; `sence=allow|deny`; `file=filename`; `item=user|tty|rhost|ruser|group|shell` `apply=user|@group`. Первый параметр задаёт возвращаемое значение в случае неудачного поиска. Второй - в случае удачного поиска. Третий - имя файла со списком. Четвёртый - тип элемента в списке. Последний вносит дополнительные ограничения, если тип объявлен «tty», «rhost» или «shell».

**pam\_mail:** Тип «auth». Сообщается о наличии почты, если таковая имеется. Полезные параметры: `dir=S` - путь к каталогу почтовых очередей, `noenv` - не устанавливать переменную среды MAIL, `close` - сообщать если есть почта у пользователей с аннулированными бюджетами, `norep` - не печатать какой-либо почтовой информации, если пользовательский бюджет только что заведён.

**pam\_nologin:** Тип «auth». Стандартная реакция на наличие файла `/etc/nologin`. Когда он присутствует, в систему может зайти только `root`, а остальным будет выдано на экран содержимое этого файла;

**pam\_permit:** Тип любой. Использование данного модуля ОПАСНО и применимо только в критических ситуациях. Всегда даёт допуск.

**pam\_pwdb:** Тип любой. Замещает модули серии «pam\_unix...» . Использует интерфейс библиотеки «libpwdb» (пользовательские базы данных), что повышает независимость системы аутентификации от способа хранения пользовательских данных (NIS или `passwd` или `shadow`). Полезные параметры: `nullok` - можно использовать пустые пароли, `md5`, `shadow`, `bigcrypt` - различные способы шифрования пароля.

**pam\_radius:** Тип «session». Позволяет осуществлять аутентификацию через RADIUS сервер.

**pam\_rhosts\_auth:** Тип «auth». Механизм работы этого модуля основывается на анализе содержимого файлов `hosts.equiv` и `.rhosts`, используемых для аутентификации таких служб как `rlogin` и `rsh`. Полезные параметры: `no_hosts_equiv` - игнорировать содержимое файла `hosts.equiv`, `no_rhosts` - игнорировать содержимое файлов `.rhosts`, `suppress` - охраняет системные журналы от потока малозначимых сообщений, в частности, когда используется контрольный флаг «sufficient».

**pam\_root\_ok:** Тип `auth`. Используется в случае, когда администратору

необходимо получать доступ к сервису без введения пароля. Этот модуль допускает пользователя к сервису только если его `uid` равен 0.

**pam\_securetty:** Включает в проверку файл `/etc/securetty`. Суперпользователь сможет зайти только на указанных там терминалах.

**pam\_time:** Тип `account`. Смотри описание устройства конфигурационного файла `time.conf`;

**pam\_warn:** Тип «`auth`» и «`password`». Просто ведёт записи в системных журналах, например, при смене пароля.

**pam\_wheel:** Тип «`auth`». Права суперпользователя может использовать только пользователь группы «`wheel`» (группа `root`). Полезные параметры: `group=XXX` - использовать указанную группу вместо стандартной нулевой, `deny` - инвертирование действия алгоритма, запрещается получать права суперпользователя пользователям указанной группы, используется вместе с предыдущим параметром, `trust` - избавляет пользователей группы «`wheel`» от необходимости вводить пароль при смене `uid` на 0.

Для отслеживания попыток неуспешной аутентификации необходимо от имени администратора `root` отредактировать файлы «`system-auth`» и «`password-auth`»:

```
vi /etc/pam.d/system-auth
vi /etc/pam.d/password-auth
```

Добавить в секцию «`auth`» две строки, устанавливающие блокировку учётной записи на время не менее 15 минут в случае ввода не более 4 неправильных паролей. И 1 строку, подключающую нужный модуль.

В PAM модулях важен порядок следования строк, поэтому структура редактируемых файлов после изменений должна быть следующая:

```
cat /etc/pam.d/password-auth
```

```
# Generated by authselect on Mon May 31 07:25:19 2021
# Do not modify this file manually.
auth required pam_env.so
auth required pam_faillock.so preauth silent audit deny=4 unlock_time=900
auth required pam_faildelay.so delay=2000000
auth [default=1 ignore=ignore success=ok] pam_usertype.so isregular
auth [default=1 ignore=ignore success=ok] pam_localuser.so
auth sufficient pam_unix.so nullok try_first_pass
auth [default=die] pam_faillock.so authfail audit deny=4 unlock_time=900
auth [default=1 ignore=ignore success=ok] pam_usertype.so isregular
auth sufficient pam_sss.so forward_pass
auth required pam_deny.so

account required pam_unix.so
account sufficient pam_localuser.so
account sufficient pam_usertype.so issystem
account [default=bad success=ok user_unknown=ignore] pam_sss.so
```

```
account required pam_permit.so
account required pam_faillock.so

password requisite pam_pwquality.so try_first_pass local_users_only
password sufficient pam_unix.so sha512 shadow nullok try_first_pass
use_authtok
password sufficient pam_sss.so use_authtok
password required pam_deny.so

session optional pam_keyinit.so revoke
session required pam_limits.so
-session optional pam_systemd.so
session [success=1 default=ignore] pam_succeed_if.so service in crond
quiet use_uid
session required pam_unix.so
session optional pam_sss.so
```

```
cat /etc/pam.d/system-auth
```

```
# Generated by authselect on Mon May 31 07:25:19 2021
# Do not modify this file manually.
auth required pam_env.so
auth required pam_faillock.so preauth silent audit deny=4 unlock_time=900
auth required pam_faildelay.so delay=2000000
auth sufficient pam_fprintd.so
auth [default=1 ignore=ignore success=ok] pam_usertype.so isregular
auth [default=1 ignore=ignore success=ok] pam_localuser.so
auth sufficient pam_unix.so nullok try_first_pass
auth [default=die] pam_faillock.so authfail audit deny=4 unlock_time=900
auth [default=1 ignore=ignore success=ok] pam_usertype.so isregular
auth sufficient pam_sss.so forward_pass
auth required pam_deny.so

account required pam_unix.so
account sufficient pam_localuser.so
account sufficient pam_usertype.so issystem
account [default=bad success=ok user_unknown=ignore] pam_sss.so
account required pam_permit.so
account required pam_faillock.so

password requisite pam_pwquality.so try_first_pass local_users_only
password sufficient pam_unix.so sha512 shadow nullok try_first_pass
use_authtok
password sufficient pam_sss.so use_authtok
password required pam_deny.so

session optional pam_keyinit.so revoke
```

```
session required pam_limits.so
-session optional pam_systemd.so
session [success=1 default=ignore] pam_succeed_if.so service in crond
quiet use_uid
session required pam_unix.so
session optional pam_sss.so
```

Здесь параметр `deny=` отвечает за число отслеживаемых неуспешных попыток, после которых произойдёт блокировка, а `unlock_time=` время в секундах, на которое учётная запись будет заблокирована.

Для многофакторной аутентификации используется модуль «`pam_usb`». Чтобы использовать FLASH-накопитель в качестве токена аутентификации, необходимо подключить к ЭВМ FLASH-накопитель и убедиться, что ОС успешно его подмонтировала.

Добавить FLASH-накопитель, который будет использоваться как токен для аутентификации:

```
pamusb-conf --add-device <Auth-Stick>
```

где `<Auth-Stick>` произвольное имя, присваиваемое токenu.

Далее необходимо выбрать устройство из числа обнаруженных:

```
Please select the device you wish to add.
* Using "JetFlash TS128MJF2A (JetFlash_TS128MJF2A-0:0)"
(only option)
Which volume would you like to use for storing data ?
```

И подтвердить его использование:

```
* Using "/dev/sdc1 (UUID: 1CD6-B3F1)" (only option)
Name      : Auth-Stick
Vendor    : JetFlash
Model     : TS128MJF2A
Serial    : JetFlash_TS128MJF2A-0:0
UUID      : 1CD6-B3F1
```

Подтвердить сохранение параметров:

```
Save to /etc/pamusb.conf ?
```

```
[Y/n] y
```

```
Done.
```

Далее необходимо добавить пользователей, которые могут использовать этот токен:

```
pamusb-conf --add-user='petrov'
```

```
Which device would you like to use for authentication ?
* Using "Auth-Stick" (only option)
User      : petrov
Device    : Auth-Stick
Save to /etc/pamusb.conf ?
```

```
[Y/n] y
```

```
Done.
```

В файлах `/etc/pam.d/system-auth` и `/etc/pam.d/password-auth` нужно в начало файла добавить строку, отвечающую за загрузку модуля, и установить уровень управляющей директивы, как было описано ранее:

```
auth sufficient pam_usb.so
```

## 6.8 Rsyslog

Rsyslog — это очень быстрый, расширяемый сервис для управления логами с огромным количеством возможностей. Среди его возможностей можно отметить поддержку фильтрации контента, а также передачу логов по сетям. Основные возможности:

- Многопоточность;
- TCP, RELP;
- Поддержка MySQL, PostgreSQL, Oracle;
- Фильтрация журналов;
- Полностью настраиваемый формат вывода.

Все программы ведут лог путём отправки сообщений об ошибках или своём состоянии с помощью сокета «syslog» или просто записывая все сообщения в файл, который будет находиться в каталоге `/var/log/`.

Но важное значение имеет уровень подробности логирования. Вы можете настраивать подробность в каждой отдельной программе, или же с помощью «syslog». Это поможет уменьшить использование дискового пространства на хранение логов. Но тут нужно найти компромисс между количеством информации и использованием диска.

Например, ядро ОС определяет такие уровни логов, или как мы будем называть их ниже — приоритеты:

- KERN\_EMERG** — система неработоспособна.
- KERN\_ALERT** — нужно немедленно принять меры.
- KERN\_CRIT** — критическая ошибка.
- KERN\_ERR** — обычная ошибка.
- KERN\_WARNING** — предупреждение.
- KERN\_NOTICE** — замечание.
- KERN\_INFO** — информационное сообщение.
- KERN\_DEBUG** — сообщения отладки.

Подобные уровни лога поддерживаются в большинстве программ, которые ведут логи.

Все настройки Rsyslog находятся в файле `/etc/rsyslog.conf` и других конфигурационных файлах из `/etc/rsyslog.d`. Вы можете посмотреть существуют ли у вас эти файлы выполнив:

```
ls /etc/rsys*  
rsyslog.conf rsyslog.d/
```

Основной конфигурационный файл — `/etc/rsyslog.conf`, в нем подключены все файлы из папки `rsyslog.d` с помощью директивы «IncludeConfig» в самом начале файла:

```
IncludeConfig /etc/rsyslog.d/*.conf
```

В этих файлах могут содержаться дополнительные настройки, например, аутентификация на Rsyslog сервере. В главном конфигурационном файле содержится очень много полезных настроек. Обычно он обеспечивает управление локальными логами по умолчанию, но для работы через сеть нужно добавить настройки.

Синтаксис конфигурационного файла очень прост:

```
<переменная> <значение>
```

Все директивы начинаются со знака доллара, содержат имя переменной, а дальше связанное с ней значение. Так выглядит каждая строка конфигурационного файла. В его первой части размещены общие настройки программы и загрузка модулей. Во второй — ваши правила сортировки и фильтрации лог файлов.

```
ModLoad imuxsock # provides support for local system logging  
$ModLoad imklog # provides kernel logging support  
#$ModLoad immark # provides --MARK-- message capability  
# provides UDP syslog reception  
#$ModLoad imudp  
#$UDPServerRun 514  
# provides TCP syslog reception  
#$ModLoad imtcp  
#$InputTCPServerRun 514
```

В этом участке загружаются все необходимые модули программы. Существуют четыре типа модулей.

- Модули ввода — можно рассматривать, как способ сбора информации из различных источников, начинаются с «im»;
- Модули вывода — позволяют отправлять сообщения в файлы или по сети, или в базу данных, имя начинается на «om»;
- Модули фильтрации — позволяют фильтровать сообщения по разным параметрам, начинаются с «fm»;

- Модули парсинга — предоставляют расширенные возможности для синтаксического анализа сообщения, начинаются с «pm».

Сначала загружается модуль «imuxsock», который позволяет сервису получать сообщения из сокета, а второй «imklog» получает сообщения ядра. Следующим загружается модуль «mark», который позволяет маркировать соединения, или же выводить сообщения о том, что «syslog» все ещё работает. Например, вы можете попросить rsyslog выводить сообщения каждые 20 минут:

```
MarkMessagePeriod 1200
```

Дальше идут глобальные директивы:

```
ActionFileDefaultTemplate RSYSLLOG_TraditionalFileFormat
```

В этой строке мы указываем, что нужно использовать стандартный формат хранения времени, в секундах с 1970 года.

Дальше следует набор прав разрешений для файлов журналов, которые будут созданы в вашей системе:

```
FileOwner root
FileGroup adm
FileCreateMode 0640
DirCreateMode 0755
Umask 0022
```

После создания этих файлов, их права можно менять на те, которые вам нужны.

Выше была более общая настройка «syslog», ну а теперь правила сортировки логов. Вот набор правил по умолчанию:

```
auth,authpriv.* - /var/log/auth.log
*.*;auth,authpriv.none - /var/log/syslog
cron.* - /var/log/cron.log
daemon.* - /var/log/daemon.log
kern.* - /var/log/kern.log
lpr.* - /var/log/lpr.log
mail.* - /var/log/mail.log
user.* - /var/log/user.log
```

Каждое правило имеет свой синтаксис, сначала идёт источник и приоритет, затем действие. Если источник и приоритет совпадают, сообщение отправляется в указанный файл. Например, мы можем отправить больше сообщений в лог системы /var/messages:

```
*.info;mail.none;authpriv.none;cron.none /var/log/messages
```

В этой строке мы выбираем все сообщения уровня info, кроме mail, authpriv и cron. Шаблон mail.none будет означать, что не нужно логировать ни один

уровень сообщений. Соответственно конструкция \*.info — значит логировать сообщения от всех источников, но только с уровнем info, \*.\* — это вообще все сообщения, со всеми уровнями.

Источник и приоритет нечувствительны к регистру. Также заметьте, что приоритеты уровней error, warn и panic больше не используются, так как считаются устаревшими. В целом, в качестве источников вы можете использовать:

- auth;
- authpriv;
- cron;
- daemon;
- kern;
- lpr;
- mail;
- mark;
- news;
- security (эквивалентно auth);
- syslog;
- user;
- uucp;
- local0 ... local7.

А в качестве приоритетов вы можете применить:

- emerg (раньше panic);
- alert;
- crit;
- error (раньше err);
- warn (раньше warning);
- notice;
- info;
- debug.

Звёздочки на любом месте означают все варианты. Для фильтрации логов могут использоваться не только источник и приоритет, но и более сложные выражения на основе условий и сравнений.

Вы можете выполнять фильтрацию сообщений с помощью такого синтаксиса:

```
:<поле>, <сравнение>, <значение> <путь_к_файлу>
```

В качестве операции сравнения вы можете использовать такие варианты:

- contains — поле содержит указанное значение;
- isequal — поле должно быть идентичным значению;
- startswith — поле должно начинаться со значения;
- regex — сравнивает поле с регулярным выражением.

Например, отфильтруем сообщения только от определённой программы:

```
:syslogtag, isequal, "giomanager:" /var/log/giomanager.log  
& stop
```

Кроме того, можно использовать более простой синтаксис, в виде выражения `if`. Вот основной синтаксис:

```
if $<поле> <сравнение> <значение> then <файл>
```

Здесь используются те же самые компоненты, только выглядит немного проще. Например:

```
if $syslogtag == 'giomanager' then /var/log/giomanager.log
```

Отправить лог на удалённый сервер достаточно просто, для этого достаточно указать `@` и `ip`-адрес удалённой машины, на которой запущен `rsyslog`:

```
*.info;mail.none;authpriv.none;cron.none @xx.xx.xx.xx:514
```

Здесь 514 — это порт, на котором слушает `rsyslog`. Настройка `rsyslog` на приём логов заключается в запуске сервиса с модулями `imtcp` и `imudp`. Далее, все что нужно для того, чтобы получить логи с определённой машины, отфильтровать их из общего потока с помощью фильтров:

```
if $fromhost-ip contains '192.168.1.10' then  
/var/log/proxyserver.log
```

Без фильтров сообщения с разных машин будут писаться в один общий лог системы в зависимости от того, как вы их распределите.

## 6.9 Afick - верификация целостности

`Afick` - это быстрая и доступная утилита, помогающая при обнаружении вторжений, а также позволяющая контролировать общую целостность системы.

`Afick` контролирует изменения в файловой системе и сразу сообщает вам о них, таким образом, предоставляя вам выбор решить, действительно ли ожидалось эти изменения. Эта информация может помочь вам в расследовании инцидента, когда необходимо определить, какие были произведены изменения в системе в результате взлома.

В процессе установки `Afick` формирует базу данных файлов, каталогов и их соответствующих им MD5 контрольных сумм. Файлы и каталоги, включенные в эту базу данных, выбираются соответственно входным данным из файла конфигурации `Afick`, называемого `afick.conf`, после того, как `Afick` установит этот файл в `/etc` каталог. Файл конфигурации `afick.conf` имеет простую синтаксическую структуру. По вашему усмотрению Вы можете очень быстро добавить или удалить типы файлов, каталоги и т.д. Ниже приведено содержимое файла `afick.conf`. Обратите внимание, что элементы в файле конфигурации чувствительны к регистру.

```
afick config sample file
```

```
# directives
#####
database:=/var/lib/afick/afick Определяет, какую базу данных будет
использовать Afick.
# report_url := stdout Определяет, куда Afick будет выводить резуль-
таты своей работы.
# verbose := no
# warn_dead_symlinks := no
# report_full_newdel := no
# warn_missing_file := no
# running_files := no
# timing := no
# text files
exclude_suffix := log LOG html htm HTM txt TXT xml Определяет, что
Afick должен игнорировать текстовые файлы с такими расширениями.
# help files
exclude_suffix := hlp pod chm Определяет, что Afick должен игнориро-
вать файлы справки с такими расширениями.
# old files
exclude_suffix := tmp old bak Определяет, что Afick должен игнориро-
вать временные файлы с такими расширениями.
# fonts
exclude_suffix := fon ttf TTF Определяет, что Afick должен игнориро-
вать файлы шрифтов с такими расширениями.
# images
exclude_suffix := bmp BMP jpg JPG gif png ico Определяет, что Afick
должен игнорировать файлы изображений с такими расширениями.
# audio
exclude_suffix := wav WAV mp3 avi Определяет, что Afick должен игно-
рировать медиа файлы с такими расширениями.
# macros
#####
# used by cron
@@define MAILTO root Определяет пользователя, которому будут отсы-
латься отчёты по работе Afick.
@@define LINES 1000 Определяет максимальное количество строк в отчё-
те.
# list the file or directories to scan
# syntaxe :
# file action
# to have action on file (see below
# ! file
# to remove file from scan
# file with blank character have to be quoted
```

```
# action : a list of item to check Ниже описаны опции, определяющие,
# какие атрибуты файлов нужно контролировать.
# md5 : md5 checksum
# d : device
# i : inode
# p : permissions
# n : number of links
# u : user
# g : group
# s : size
# b : number of blocks
# m : mtime
# c : ctime
# a : atime
#R: p+d+i+n+u+g+s+m+c+md5
#L: p+d+i+n+u+g
# action alias may be configured with
# your_alias = another_alias|item[+item] [-item]
# all is a pre-defined alias for all items except "a"
# alias :
#####
DIR = p+i+n+u+g
ETC = p+d+i+u+g+s+md5
Logs = p+n+u+
MyRule = p+d+i+n+u+g+s+b+md5+m .
# files to scan
#####
=/ DIR Проверка с использованием описанных выше правил для каталогов.
#
/bin MyRule
/boot MyRule
!/boot/map Игнорируется указанный каталог.
!/boot/System.map Игнорируется указанный файл.
/etc ETC
/etc/mtab ETC - i
/etc/adjtime ETC - md5
/etc/aliases.db ETC - md5
/etc/mail/statistics ETC - md5
!/etc/map
!/etc/webmin/sysstats/modules/
!/etc/cups/certs/0
/lib MyRule
/lib/modules MyRule -m
/root MyRule
!/root/.viminfo
```

```
!/root/.bash_history
!/root/.mc
/sbin MyRule
/usr/bin MyRule
/usr/sbin MyRule
/usr/lib MyRule
/usr/local/bin MyRule
/usr/local/sbin MyRule
/usr/local/lib MyRule
/var/ftp MyRule
/var/log Logs
/var/www MyRule
```

Как видно, файл конфигурации Afick довольно прост для понимания. Ниже приведён пример, в котором к проверке целостности Afick добавляется ваш основной каталог. К примеру, вам необходимо, чтобы файлы в этом каталоге проверялись на изменения при монопольном доступе, изменение прав доступа, изменения размера файлов и времени последнего обращения к файлу. Для начала нужно создать новый элемент, под разделом #alias в файле конфигурации afick.conf, как показано ниже:

```
HOME = u+g+p+m+s
```

Затем в разделе #files to scan необходимо добавить следующую строку:

```
/home/yourusername HOME
```

Теперь, при следующем запуске, Afick добавит ваш каталог в свою базу данных и будет контролировать находящиеся в нем файлы, согласно указанным вами критериям. Если вы хотите, чтобы ваши изменения применились немедленно, то можно запустить Afick вручную, используя следующую команду:

```
Afick -- update
```

Иначе, вам придётся ждать запуска крон задачи Afick. Эта задача добавляется автоматически во время инсталляции программы и запускается один раз в день. Результаты работы данного задания вы получите по электронной почте на адрес, указанный в разделе <MAILTO> файла конфигурации «afick.conf». Используя почтового клиента, вы сможете увидеть ежедневный отчёт примерно в таком виде:

```
This is an automated report generated by Another File Integrity
Checker on
+localhost.localdomain at 07:46:07 AM on 02/25/2004.
Output of the daily afick run:
new file : /var/log/afick/afick.log.2
new file : /var/log/afick/error.log.2
```

```
deleted file : /etc/sysconfig/iptables
changed file : /etc/adjtime
changed file : /etc/aliases.db
changed file : /etc/mail/statistics
changed file : /etc/prelink.cache
changed file : /etc/printcap
detailed changes
changed file : /etc/adjtime
MD5 : 7+bTDZQbxsTXEJXhyI2GCw ао6а/yDwoBR8GSL1AK1WXQ
changed file : /etc/aliases.db
MD5 : GT/eP5D+B8apNoa7L5CLRw soh7MnLDuQw4gI9KH1hpTA
changed file : /etc/mail/statistics
MD5 : oshq17jZ2a0o5pYhVBRgwQ vb69gMWXvpIEEZ4fm019/Q
changed file : /etc/prelink.cache
MD5 : SKh/403FRMUqBNdCIInQ9A zeC+5EPFfWBR40eT7xZdbw
changed file : /etc/printcap
MD5 : b5e3g2//bGaxeCxVyRJqaw QFY1NJGy/kdt32B1YVOTXQ
filesize : 194 581
```

В примере выше Afick сообщает нам, что некоторые файлы были изменены, созданы или удалены. Также нам показываются начальные и текущие контрольные суммы файлов, и сообщается, что в одном из файлов был изменён его размер. Afick узнает о происходящих изменениях в файле, сравнивая его атрибуты с атрибутами, которые были сохранены при последнем запуске Afick. Примером этого могут служить файлы в папке `/usr/bin` или в `/sbin`. Обычно эти файлы редко изменяются, если только вы не изменили их, обновляя программу (в противном случае они не должны изменяться).

Обратите внимание на то, где вы сохраняете вашу базу данных Afick (по умолчанию - `/var/lib/afick/`), потому что может возникнуть ситуация, когда ваша система была взломана, а вы об этом не узнаете, т.к. была нарушена целостность базы данных. Возможным решением данного вопроса может быть сохранение базы на защищённых от записи носителях (например, CD-ROM), после чего следует изменить файл конфигурации «`afick.conf`», чтобы указать на выбранное вами место сохранения базы.

## 6.10 AMTU - утилита тестирования абстрактной машины

`amtu` — утилита тестирования абстрактной машины (Abstract Machine Test Utility — AMTU).

Синтаксис:

```
amtu [ -dmsinph ]
```

AMTU - это административная утилита, которая проверяет, соблюдаются ли основные механизмы защиты аппаратного обеспечения.

AMTU выполняет следующие тесты:

- **память:** произвольно записывает данные в области памяти, затем считывает память, чтобы гарантировать, что записанные значения остаются

неизменными;

- **разделение памяти:** обеспечивает, чтобы программы пользовательского пространства не могли читать и записывать в области памяти, используемые такими элементами, как видеопамять и код ядра;
- **контроллер ввода / вывода — сеть:** проверяет, что переданные случайные данные также являются данными, полученными для каждого настроенного сетевого устройства. Проверяет только настроенные устройства Ethernet и Token Ring. Не проверяет асинхронные устройства;
- **контроллер ввода / вывода — диск:** проверяет, что случайные данные, записанные на диски, остаются неизменными. Проверяются только контроллеры IDE и SCSI, связанные с установленными файловыми системами. Контроллеры дисков с файловыми системами, доступными только для чтения, не проверяются;
- **инструкции режима супервизора:** обеспечивает, что принудительное использование свойств привилегированных инструкций в режиме супервизора по-прежнему действует. Набор привилегированных инструкций, проверенных для подтверждения этого, зависит от архитектуры.

Для команды `amtu` доступны следующие параметры:

Параметр	Значение параметра
<code>-d</code>	выводить отладочные сообщения;
<code>-m</code>	выполнить проверку памяти;
<code>-s</code>	выполнить проверку разделения памяти;
<code>-i</code>	выполнить тест контроллера ввода-вывода;
<code>-n</code>	выполнить сетевой тест;
<code>-p</code>	выполнить проверку инструкций режима супервизора;
<code>-h</code>	показать справку.

Команда `amtu` выдаёт следующие коды возврата при выполнении:

- «-1» — ошибка выполнения;
- «0» — успех.

## 6.11 ntpdate

В РЕД ОС синхронизировать время можно следующими основными способами:

- вручную утилиты `ntpdate`;
- автоматически при помощи сервиса `ntp`.

Программа `ntpdate` — позволяет разово синхронизировать локальное время с эталонным сервером времени в интернете. Подобных эталонов существует достаточно много. Для примера можно воспользоваться одним из них — `pool.ntp.org`

Запускаем синхронизацию времени:

```
ntpdate pool.ntp.org
```

Утилита провела синхронизацию, в результате которой к системному времени было добавлено число секунд, необходимое для приближения к эталонному. Если в результате работы синхронизации возникает ошибка: «no server suitable for synchronization found», то попробуйте в работе утилиты использовать непривилегированный порт. По-умолчанию ntpdate работает по 123 порту. Если он закрыт на фаерволе, то помочь в синхронизации поможет следующий параметр:

```
ntpdate -u pool.ntp.org
```

Если у вас запуск ntpdate завершается ошибкой — the NTP socket is in use, exiting, значит у вас уже установлена и запущена служба ntpd, которая заняла свободный udp порт, необходимый для работы ntpdate.

Сервер времени ntp использует в своей работе одноимённый протокол — Network Time Protocol, которому для работы необходим UDP порт 123. Так что перед установкой и настройкой службы времени убедитесь, что на фаерволе открыт этот порт.

Устанавливаем сервер ntp:

```
dnf -y install ntp
```

Теперь отредактируем файл конфигурации /etc/ntp.conf , удалив все лишнее:

```
cat /etc/ntp.conf
```

```
driftfile /var/lib/ntp/drift
restrict default nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict ::1
server 0.centos.pool.ntp.org iburst
server 1.centos.pool.ntp.org iburst
server 2.centos.pool.ntp.org iburst
server 3.centos.pool.ntp.org iburst
disable monitor
logfile /var/log/ntp.log
```

Параметры:

**server** - список серверов для синхронизации времени;

**driftfile** – задаёт адрес файла, в котором хранится история изменений времени во время синхронизации. Если по каким-то причинам синхронизация времени с внешними источниками станет невозможна, служба времени изменит системные часы в соответствии с записями в этом файле;

**restrict 127.0.0.1** – указывает, что пользоваться нашим сервером времени можно только непосредственно с локального интерфейса. Если вам необходимо разрешить другим компьютерам в вашей локальной сети синхронизировать

время с текущей машины, то укажите в данном параметре адрес вашей сети, например:

```
restrict 192.168.10.0 mask 255.255.255.0
```

**restrict default nomodify notrap nopeer noquery** – параметры указывают на то, что клиентам данного сервиса времени запрещено изменять его настройки, получать его статус. Они могут только забрать с него значения точного времени;

**disable monitor** – данный параметр повышает безопасность, предотвращая использования одной из уязвимостей сервиса ntpd, которую можно использовать для проведения DDoS-атак;

**logfile** – указывает путь к файлу с логами сервиса.

После завершения редактирования файла настроек запускаем службу синхронизации времени:

```
systemctl start ntpd
```

Проверяем запустился ли сервер:

```
netstat -tulnp | grep 123
```

Все в порядке, служба слушает положенный порт 123. Проверим ещё на всякий случай системные логи ОС:

```
cat /var/log/messages | grep ntpd  
cat /var/log/ntp.log
```

Теперь настроим автозапуск ntp вместе с загрузкой ОС:

```
systemctl enable ntpd
```

Наблюдать за работой службы ntp можно с помощью команды:

```
ntpq -p
```

Данные вывода:

**remote** – адрес удалённого эталона времени, с которого была синхронизация;

**refid** – указывает, откуда каждый эталон получает точное время. Это могут быть другие сервера времени, система GPS и другое;

**st** (stratum (уровень)) – это число от 1 до 16, которое указывает на точность эталона. «1» - максимальная точность, «16» — сервер недоступен. Уровень вашего сервера будет равен уровню наименее точного удалённого эталона плюс 1;

**poll** – интервал в секундах между опросами;

**reach** – восьмеричное представление массива из 8 бит, отражающего результаты последних восьми попыток соединения с эталоном. Бит выставлен, если удалённый сервер ответил;

**delay** – время задержки ответа на запрос о точном времени;

**offset** – разница между вашим и удаленным сервером;

**jitter** – дисперсия – это мера статистических отклонений от значения смещения (поле **offset**) по нескольким успешным парам запрос-ответ. Чем меньше значение дисперсии, тем лучше, поскольку позволяет точнее синхронизировать время.

## 6.12 Отказоустойчивый кластер

Corosync - это программа с открытым исходным кодом, которая предоставляет возможности кластерного членства и обмена сообщениями, часто называемые уровнем обмена сообщениями, на клиентские серверы. Расemaker - это менеджер ресурсов кластера с открытым исходным кодом (CRM), который координирует ресурсы и службы, которые управляются и становятся доступными кластеру. По сути, Corosync позволяет серверам связываться как кластер, в то время как Расemaker предоставляет возможность управлять тем, как ведёт себя кластер.

Архитектура расemaker состоит из трёх уровней:

- Кластеронезависимый уровень – на этом уровне располагаются сами ресурсы и их скрипты, которыми они управляются и локальный демон, который скрывает от других уровней различия в стандартах, использованных в скриптах.
- Менеджер ресурсов (Расemaker), который представляет из себя мозг. Он реагирует на события, происходящие в кластере: отказ или присоединение узлов, ресурсов, переход узлов в сервисный режим и другие административные действия. Расemaker, исходя из сложившейся ситуации, делает расчёт наиболее оптимального состояния кластера и даёт команды на выполнение действий для достижения этого состояния (остановка/перенос ресурсов или узлов).
- Информационный уровень – на этом уровне осуществляется сетевое взаимодействие узлов, т.е. передача сервисных команд (запуск/остановка ресурсов, узлов и т.д.), обмен информацией о полноте состава кластера (**quorum**) и т.д. На этом уровне работает Corosync.

Для наглядности рассмотрим создание простого кластера с плавающим ip-адресом. В случае если работающий сервер отказывается, второй автоматически запускается и начинает работать вместо первого.

Если вы хотите иметь доступ к настройкам кластера через доменное имя, необходимо настроить DNS-адресацию серверов. Если у вас нет имени домена для использования, можно использовать плавающий IP-адрес для доступа к настройкам.

Всякий раз, когда есть несколько серверов, обменивающихся друг с другом информацией, особенно с помощью программного обеспечения для кластеризации, важно обеспечить синхронизацию их часов. Рекомендуется использовать NTP (Network Time Protocol) для синхронизации серверов.

Corosync использует UDP-транспорт между портами 5404 и 5406 . Если вы используете брандмауэр, убедитесь, что между этими серверами разрешена связь.

Установка Corosync и Расemaker:

```
dnf install corosync pcs pacemaker
```

Для управления кластером рекомендуется пользоваться утилитой pcs. При установке pacemaker автоматически будет создан пользователь hacluster. Для использования pcs, а также для доступа в веб-интерфейс нужно задать пароль пользователю hacluster:

```
passwd hacluster
Changing password for user hacluster.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Запуск сервиса:

```
systemctl start pcsd
```

Настраиваем аутентификацию (на одном узле):

```
pcs cluster auth <Сервер1> <Сервер2>
Username: hacluster
Password:
<Сервер1>: Authorized
<Сервер2>: Authorized
```

Вместо имён <Сервер1> и <Сервер2> используйте ваши доменные имена серверов.

После этого кластером можно управлять с одного узла.

Создаём кластер:

```
pcs cluster setup --name mycluster <Сервер1> <Сервер2>
```

```
Shutting down pacemaker/corosync services...
Redirecting to /bin/systemctl stop pacemaker.service
Redirecting to /bin/systemctl stop corosync.service
Killing any remaining services...
Removing all cluster configuration files...
<Сервер1>: Succeeded
<Сервер2>: Succeeded
Synchronizing pcsd certificates on nodes <Сервер1>, <Сервер2>...
<Сервер1>: Success
<Сервер2>: Success
Restarting pcsd on the nodes in order to reload the certificates..
<Сервер1>: Success
<Сервер2>: Success
```

Запускаем кластер:

```
pcs cluster start --all
```

```
<Сервер2>: Starting Cluster...  
<Сервер1>: Starting Cluster...
```

Настройка автоматического включения кластера при загрузке:

```
pcs cluster enable --all
```

```
<Сервер1>: Cluster Enabled  
<Сервер2>: Cluster Enabled
```

Смотрим результат:

```
pcs status cluster
```

```
Cluster Status:  
Stack: unknown  
Current DC: NONE  
2 nodes and 0 resources configured  
Node <Сервер1>: UNCLEAN (offline)  
Node <Сервер2>: UNCLEAN (offline)  
PCSD Status:  
<Сервер1>: Online  
<Сервер2>: Online
```

Проверка синхронизации узлов кластера:

```
corosync-smapctl | grep members
```

```
runtime.totem.pg.mrp.srp.members.1.config_version (u64) = 0  
runtime.totem.pg.mrp.srp.members.1.ip (str) = r(0)  
ip(192.168.100.201)  
runtime.totem.pg.mrp.srp.members.1.join_count (u32) = 1  
runtime.totem.pg.mrp.srp.members.1.status (str) = joined  
runtime.totem.pg.mrp.srp.members.2.config_version (u64) = 0  
runtime.totem.pg.mrp.srp.members.2.ip (str) = r(0)  
ip(192.168.100.202)  
runtime.totem.pg.mrp.srp.members.2.join_count (u32) = 1  
runtime.totem.pg.mrp.srp.members.2.status (str) = joined  
pcs status corosync  
Membership information  
-----  
Nodeid Votes Name  
1 1 <Сервер1> (local)
```

```
2 1 <Сервер2>
```

Настройка основных параметров кластера.

Механизм STONITH (Shoot-The-Other-Node-In-The-Head) — защита от Split-Brain : позволяет выключать/включать/перезагружать узлы кластера. Обычно этот механизм реализуется с помощью специальных сетевых устройств с удаленным управлением или через специальные платы управления сервером. В расемAKER устройства STONITH реализованы в виде кластерных ресурсов.

Кворум определяет минимальное число работающих узлов в кластере, при котором кластер считается работоспособным. По умолчанию, кворум считается неработоспособным, если число работающих узлов меньше половины от общего числа узлов. Так как узла у нас всего два, то кворума у нас не будет, поэтому необходимо отключить эту политику:

```
pcs property set no-quorum-policy=ignore
```

Посмотреть какие получились настройки можно командой:

```
pcs property
```

```
Cluster Properties:
cluster-infrastructure: corosync
cluster-name: mycluster
dc-version:
have-watchdog: false
last-lrm-refresh: 1480973783
no-quorum-policy: ignore
stonith-enabled: false
```

Настройки кластера можно проверить с помощью утилиты «crm\_verify». Опция «-L» осуществляет диагностику всех работающих узлов кластера.

Чтобы сервисы кластера запускались автоматически при перезагрузке сервера, нужно выполнить на каждом узле кластера:

```
systemctl enable pcsd
systemctl enable corosync
systemctl enable pacemaker
```

Создание виртуального плавающего ip-адреса (floatingip) VIP:

```
pcs resource create virtual_ip ocf:heartbeat:IPaddr2
ip=192.168.100.203 cidr_netmask=32 op monitor interval=30s
pcs status resources
virtualip (ocf::heartbeat:IPaddr2): Started <Сервер1>
```

Если узлы кластера не одинаковы по производительности или доступности, то можно увеличить приоритет одного из узлов, чтобы он был активным всегда когда работает:

```
pcs constraint location virtualip prefers <Сервер1>=100
```

Настройка сервисов, ресурсов и прочего производится согласно документации, поставляемой разработчиком приложения, и может быть найдена в открытых источниках в глобальной сети Интернет и на сайте разработчика.

### 6.13 Изменение приоритета процесса

Утилита `nice` — программа, предназначенная для запуска процессов с изменённым приоритетом `nice`. Приоритет `nice` (целое число) процесса используется планировщиком процессов ядра ОС при распределении процессорного времени между процессами.

Приоритет `nice` — число, указывающее планировщику процессов ядра ОС приоритет, который пользователь хотел бы назначить процессу.

Утилита `nice`, запущенная без аргументов, выводит приоритет `nice`, унаследованный от родительского процесса. `nice` принимает аргумент «смещение» в диапазоне от  $-20$  (наивысший приоритет) до  $+19$  (низший приоритет). Если указать смещение и путь к исполняемому файлу, утилита `nice` получит приоритет своего процесса, изменит его на указанное смещение и использует системный вызов семейства `exec()` для замещения кода своего процесса кодом из указанного исполняемого файла. Команда `nice` сделает то же, но сначала выполнит системный вызов семейства `fork()` для запуска дочернего процесса (англ. `sub-shell`). Если смещение не указано, будет использовано смещение  $+10$ . Привилегированный пользователь (`root`) может указать отрицательное смещение.

Приоритет `nice` и приоритет планировщика процессов ядра ОС — разные числа. Число `nice` — приоритет, который пользователь хотел бы назначить процессу. Приоритет планировщика — действительный приоритет, назначенный процессу планировщиком. Планировщик может стремиться назначить процессу приоритет, близкий к `nice`, но это не всегда возможно, так как в системе может выполняться множество процессов с разными приоритетами. Приоритет `nice` является атрибутом процесса и, как и другие атрибуты, наследуется дочерними процессами. В выводе утилит `top`, `ps`, `htop` и др. приоритет `nice` называется «NI» — сокращение от «`nice`», а приоритет планировщика — «PRI» — сокращение от «`priority`». Обычно,  $NI = PRI - 20$ , но это верно не всегда. По умолчанию  $NI=0$ , соответственно  $PRI=20$ .

Планировщик процессов ядра ОС поддерживает приоритеты от 0 (реальное время) до 139 включительно. Приоритеты  $-20 \dots +19$  утилиты или команды `nice` соответствуют приоритетам  $100 \dots 139$  планировщика процессов. Другие приоритеты планировщика процессов можно установить командой «`chrt`» из пакета «`util-linux`».

Для изменения приоритета уже запущенных процессов используется утилита `renice`.

Синтаксис:

```
nice [-n <смещение>] [--adjustment=<смещение>]  
[<команда> [<аргумент...>]]
```

Параметры:

- `-n <смещение>`;
- `--adjustment=<смещение>`.

Установить приоритет `nice`, равный сумме текущего приоритета `nice` и указанного числа `<смещение>`. Если этот аргумент не указан, будет использовано число 10.

Чтобы запустить процесс со значением `nice`, отличным от 10, можно использовать ключ `-n`.

```
nice -n 15 yes > /dev/null &
```

или

```
nice -15 yes > /dev/null &
```

Чтобы установить значение `nice` ниже нуля, требуются права суперпользователя. В противном случае будет установлено значение «0». Попробуем задать значение `nice` «-1» без прав `root`:

```
nice -n -1 yes > /dev/null &  
nice: cannot set niceness: Permission denied
```

Поэтому, чтобы задать значение `nice` меньше 0, необходимо запускать программу как `root`, или использовать `sudo`.

```
nice -n -1 yes > /dev/null &
```

У запущенной программы с помощью команды `renice` можно изменить назначенный приоритет. Предположим, что есть работающая программа «yes» со значением `nice` 10. Чтобы изменить его значение, можно использовать команду «`renice`» со значением `nice` и PID процесса. Изменим значение `nice` на 15:

```
renice -n 15 -p 5645
```

Согласно правилам, обычный пользователь может только увеличивать значение `nice` (уменьшать приоритет) любого процесса. Если попробовать изменить значение `nice` с 15 до 10, мы получим следующее сообщение об ошибке:

```
renice -n 10 -p 5645
```

```
renice: failed to set priority for 5645 (process ID):  
Permission denied
```

Также, команда `renice` позволяет суперпользователю изменять значение `nice` процессов любого пользователя. Это делается с помощью ключа «-u». Следующая команда изменяет значение приоритета всех процессов пользователя на -19:

```
renice -n -19 -u lubos
```

```
1000 (user ID) old priority 0, new priority -19
```

## 6.14 Управление дисковыми квотами

Система `diskquota` обеспечивает механизм для управления используемым дисковым пространством. Ограничения могут быть установлены для каждого пользователя в отдельности, для любой или для всех файловых систем. Система ограничений (`quota`) будет предупреждать пользователей, когда они превысят свой дозволенный лимит, но будет позволять использовать некоторое дополнительное пространство для текущей работы. Система ограничений (`quota system`) является частью ядра ОС.

Команда:

```
quota
```

позволяет просмотреть любые ограничения дискового пространства для каждого пользователя.

Доступны два типа ограничений, которые могут быть наложены на пользователя, обычно если используется одно из ограничений, то и второе тоже будет использоваться. Ограничение может быть установлено как на все дисковое пространство пользователя, которое используется этим пользователем, так и на число файлов (`inodes`), которыми он может владеть. `Quota` обеспечивает информацию на ограничения, которые были установлены системным администратором, на каждую из областей, которые используются в данный момент. Ограничения по `inodes` и `block` накладываются как на `uid` (идентификатор пользователя), так и на `gid` (идентификатор группы). Так если вы входите в группу, которая превысила наложенное на неё ограничение, то вы не сможете использовать дисковое пространство, даже если вы все ещё можете использовать его как пользователь.

Существуют четыре числа для каждого ограничения:

- используемое в данное время ограничение;
- «мягкое» ограничение (`softlimit`);
- «жесткое» ограничение (`hardlimit`);
- промежуток времени, после истечения которого «мягкое» ограничение интерпретируется как «жесткое».

«Мягкое» ограничение определяет число блоков размером 1 Кбайт, которое пользователь может немного превысить. «Жесткое» ограничение не может быть превышено ни каким образом. Если пользователь пытается превысить данное число, то он получает сообщение о невозможности сделать это. При этом ядро возвращает код ошибки `EDQUOT`. После того как пользователь превысит доступное для него «мягкое» ограничение (`softlimit`) устанавливается время, после истечения которого «мягкое» ограничение становится «жестким» (`hardlimit`). Обычно срок этого периода истекает после 7 дней (1 неделя). В этот период времени пользователь может удалить ненужные ему файлы, после чего он вновь может использовать «мягкое» ограничение до момента истечения указанного

промежутка времени. После истечения указанного промежутка времени «мягкое» ограничение становится «жестким» ограничением и у пользователя больше нет ресурсов для создания новых файлов.

Для того чтобы установить систему ограничений дискового пространства (quota) в ОС, системному администратору необходимо сделать несколько шагов:

- выбрать файловую систему, на которую будут накладываться ограничения;
- разрешить (включить) систему ограничений;
- произвести проверку файловой системы на ограничения дискового пространства;
- произвести проверку ограничений дискового пространства как для пользователей, так и для групп;
- запретить ограничения для пользователей и групп.

В первую очередь необходимо решить, на какую файловую систему необходимо наложить ограничения (quotas). Чаще всего ограничения накладываются на файловую систему, в которой располагаются домашние каталоги пользователей или на файловую систему, которая смонтирована в каталог /usr, и пользователи имеют право записывать на неё информацию. Для того чтобы разрешить ограничения на дисковое пространство, на необходимой файловой системе вы должны отредактировать файл /etc/fstab, добавив к указанной системе опции для ограничения дискового пространства (как для пользователей, так и для групп).

Отредактированный файл /etc/fstab может иметь вид:

```
#
# /etc/fstab
#
/dev/hda1 / ext2 defaults
/dev/hda2 none swap sw
/dev/hda3 /usr ext2 defaults
/dev/hdb1 /usr/users ext2 defaults,usrquota,grpquota
/dev/hdb2 /usr/src ext2 defaults,usrquota
none /proc proc defaults
```

Зарезервированное слово «usrquota», в поле опций включает ограничение дискового пространства (quotas) для пользователей (userquota) на данном устройстве. Зарезервированное слово «grpquota» включает ограничение дискового пространства для групп (groupquota) на данном устройстве. Во то время когда вы используете опции «usrquota» и «grpquota» без «=», ваши файлы ограничений (quotafile) будут находиться в корневом каталоге каждой файловой системы, в которой используются ограничения на дисковое пространство. Файл называемый «quota.user» будет использоваться для ограничений пользователей, а файл «quota.group» будет использоваться для ограничений групп. Однако, вы сами можете определить ваши файлы ограничений.

Например, строка «usrquota=/usr/adm/quotasrc.user» установит файл ограничений для пользователей в каталоге /usr/adm, который будет назы-

ваться «quotarc.user». Однако, будьте внимательны, и отслеживайте длину строки в файле /etc/fstab (смотрите ее определение в файле mntent.h).

Периодически (в основном после некорректной перезагрузки системы и во время первого разрешения ограничений на дисковое пространство) записи, содержащиеся в файле ограничений, должны быть проверены на целостность действительного числа блоков и файлов, выделенных для пользователя. Для выполнения этой операции может быть использована команда «quotacheck».

Данную команду необязательно выполнять для неподмонтированных файловых систем или в файловых системах, на которых отключено ограничение на дисковое пространство (quotas). Для проверки файловой системы на число блоков, используемых пользователем, а так же для установки и изменения всех файлов ограничений (quotafiles), выполните команду:

```
quotacheck -avug
```

Вы можете вставить данную команду в один из rc-скриптов и запускать ее на файловой системе так же как и fsck, только тогда, когда не установлен флаг «fastreboot». Данная программа не поддерживает одновременную параллельную проверку нескольких файловых систем. Для того чтобы включить систему ограничений на дисковое пространство на вашем компьютере, добавьте строку

```
/usr/bin/quotaoon -avug
```

в один из ваших /etc/rc файлов. Данная команда будет включать поддержку ограничений дискового пространства во время загрузки вашей системы.

Только суперпользователь может использовать команду «quota» для проверки используемых ограничений любого пользователя и команду «repquota» для проверки используемого пространства и ограничений для всех пользователей на данной файловой системе.

Для того чтобы получить информацию об ограничениях, наложенных на всех пользователей, необходимо выполнить команду:

```
repquota -ua
```

После чего на экране можно будет видеть таблицу, в которой указаны ограничения, наложенные на каждого пользователя. Содержимое экрана после выполнения вышеприведенной команды может иметь вид:

```
Block limits File limits
User used soft hard grace used soft hard grace
root -- 487082 0 0 12147 0 0
daemon -- 399 0 0 2 0 0
news -- 626 0 0 46 0 0
```

Для получения информации о группах необходимо выполнить команду:

```
repquota -ga
```

Для редактирования ограничения дискового пространства необходимо использовать программу «edquota». Для редактирования ограничений дискового пространства для конкретного пользователя необходимо использовать программу «edquota» с опцией «-u», а для группы необходимо использовать ту же программу, но с опцией «-g». Редактировать необходимо только число, которое следует за словом «hard» или «soft». Например, после выполнения команды:

```
edquota -u cola
```

содержимое экрана может иметь вид:

```
Quotas for user cola:  
/dev/hdb3: blocks in use: 345, limits (soft = 1, hard = 0)  
inodes in use: 94, limits (soft = 0, hard = 0)
```

После чего вы можете изменить значения, указанные после слов «hard» и «soft». При редактировании используется редактор, который указывается в переменной окружения EDITOR.

Для каждой файловой системы, имеющей ограничение на дисковое пространство, вы видите две строки. Слово «soft» означает, что на данную файловую систему наложено «мягкое» ограничение (softlimit), при этом пользователь или группа имеют некоторый интервал времени (grace period), в течении которого они могут превысить указанное значение. Данный интервал времени можно изменить с помощью команды:

```
edquota -t
```

Например, после выполнения данной команды, содержимое экрана может иметь вид:

```
Time units may be: days, hours, minutes, or seconds  
Grace period before enforcing soft limits for users:  
/dev/hdb3: block grace period: 10 minutes, file grace period:  
10 minutes
```

После чего вы можете изменить значения, указанные по умолчанию. По умолчанию используется значение, определённое в файле LINUX quota.h. Если пользователь или группа не удалят лишних файлов в течение указанного периода времени, то данные файлы переходят в разряд «жестких» ограничений (hardlimit). Слово «hard» означает, что на данную файловую систему наложено «жёсткое» ограничение. Жёсткое ограничение является максимальным значением, которое может иметь пользователь или группа на данной файловой системе. Пользователь или группа не могут иметь больше файлов или inodes, чем указано в «hard».

Строка

```
/dev/hdb3: blocks in use: 345, limits (soft = 1, hard = 0)
```

сообщает, какое число блоков может быть выделено для данного пользователя или группы.

Строка

```
inodes in use: 94, limits (soft = 0, hard = 0)
```

сообщает, какое число inode (файлов, устройств, поименованных каналов (pipes) и т.д.) может быть выделено для данного пользователя или группы.

В большинстве случаев вам приходится иметь группу пользователей, которые должны иметь одинаковые ограничения на дисковое пространство на указанной файловой системе. Самый быстрый путь отредактировать ограничения на дисковое пространство для этих пользователей заключается в создании прототипа одного из пользователей или группы для всех других. Вам нужно с помощью команды:

```
edquota -u <имя_пользователя/группы_который_станет_прототипом>
```

отредактировать ограничения на дисковое пространство, после чего с помощью команды:

```
edquota -p <имя_прототипа>*
```

отредактировать ограничения для всех оставшихся пользователей.

Например, для того чтобы в качестве ограничений дискового пространства (quota) для пользователя ola использовались ограничения, наложенные на пользователя cola, вам необходимо выполнить команду:

```
edquota -p cola ola
```

Для проверки ограничений дискового пространства для пользователя и группы используется программа quota.

Синтакс этой программы:

```
quota [-guqv]
quota [-qv] -u <username> ...
quota [-qv] -g <groupname> ...
```

Используйте опцию «-v» для вывода информации о:

- файловых системах, которые не имеют включёнными ограничения на дисковое пространство (quota),
- файловых системах, на которых вы уже установили систему ограничения дискового пространства, но на которых ещё не занят ни один блок.

Используйте опцию «-q» для просмотра файловых систем, на которых превышено значение «мягкого» (softlimit) и «жесткого» (hardlimit) ограничения.

Опция «-g» даёт вам возможность просмотреть все ограничения, которые наложены на группы, членом которых вы являетесь.

Например, с помощью команды:

```
quota -u cola
```

вы можете получить информацию об ограничениях дискового пространства, которые наложены на пользователя cola. Содержимое экрана после выполнения данной команды может иметь вид:

```
Disk quotas for user cola (uid 1002):
Filesystem blocks quota limit grace files quota limit grace
/dev/hdb3 345* 1 0 none 94 0 0
```

Если вы захотели запретить ограничения, наложенные на какого-то пользователя или на группу, то вам необходимо воспользоваться программой «edquota» для редактирования значений «hard» и «soft». Установите эти значения в 0. После чего для данного пользователя или группы не будет существовать ограничений на дисковое пространство, и он/она сможет создавать неограниченное количество файлов (ограниченное только дисковым пространством).

## 6.15 Ограничение ресурсов пользователя

Для ограничения ресурсов, доступных пользователю, используется конфигурационный файл `/etc/security/limits.conf`. Для включения лимитов необходимо добавить библиотеку PAM `pam_limits.so` в соответствующем модуле. Например:

```
session required pam_limits.so
```

в файле `/etc/pam.d/login`.

Для изменения лимитов редактируем файл `/etc/security/limits.conf`. Формат файла:

```
<группа>/<пользователь> <лимит>(жёсткий/мягкий) <параметр>
<значение>
```

Описание параметров:

**core** - размер core файлов (KB);

**data** - максимальный размер данных (KB);

**fsize** - максимальный размер файла (KB);

**memlock** - максимальное заблокированное адресное пространство (KB);

**nofile** - максимальное количество открытых файлов;

**rss** - максимальный размер памяти для резидент-программ (KB);

**stack** - максимальный размер стека (KB);

**cpu** - максимальное процессорное время (MIN);

**nproc** - максимальное количество процессов;

**as** - ограничение адресного пространства (KB);

**maxlogins** - максимальное число одновременных регистраций в системе;

**maxsyslogins** - максимальное количество учётных записей;

**priority** - приоритет запущенных процессов;  
**locks** - максимальное количество блокируемых файлов пользователем;  
**sigpending** - максимальное количество сигналов, которые можно передать процессу;  
**msgqueue** - максимальный размер памяти для очереди POSIX сообщений (bytes);  
**nice** - максимальный приоритет, который можно выставить: [-20, 19];  
**rtprio** - максимальный приоритет времени выполнения;  
**chroot** - изменить директорию root'a (Debian-specific).  
Вместо групп/пользователя можно использовать групповой символ \* (для всех) и групповой символ % для wildcard'a групп.

## 6.16 Контроль целостности запускаемых компонентов программного обеспечения

Для контроля целостности компонентов ОС используется IMA. Компонент архитектуры измерения целостности (IMA) выполняет проверки целостности во время выполнения файлов с использованием хэшей, сравнивая их со списком допустимых хэшей.

Установить утилиты для работы с IMA:

```
dnf install ima-manage keyutils attr
```

Для использования контроля целостности администратор системы должен создать секретный ключ (key.pem) и подписанный запрос на сертификат командой:

```
openssl req -new -newkey rsa:2048 -keyout <path to secret  
key.pem> -nodes -out <path to request>
```

Необходимо заполнить предлагаемые поля. Пример заполнения приведён ниже:

```
openssl req -new -newkey rsa:2048 -keyout /tmp/skey.pem -nodes  
-out /tmp/req
```

```
Generating a 2048 bit RSA private key  
.....+++  
.....+++  
writing new private key to '/tmp/skey.pem'  
-----  
You are about to be asked to enter information that will be  
incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished  
Name or a DN.
```

```

There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:ru
State or Province Name (full name) []:vladimir
Locality Name (eg, city) [Default City]:murom
Organization Name (eg, company) [Default Company Ltd]:000
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:server
Email Address []:test@test.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:

```

После успешного формирования необходимо отправить запрос полученный на предыдущем шаге <request> разработчику. В ответ на запрос разработчики предоставят сертификат (x509\_evm.der).

Далее необходимо разместить полученный сертификат в каталог /etc/keys/, а ключ сохранить в каталоге, недоступном для всех пользователей, кроме администратора root, например: /root/.

Изменить в функции check() в файле /usr/lib/dracut/modules.d/98ima/module-setup.sh return 255 на return 0:

```

# called by dracut
check() {
return 0
}

```

Произвести регенерацию initramfs:

```
dracut -f -v
```

Перезагрузить ЭВМ.

Проверить корректность загрузки сертификатов:

```
keyctl show %keyring:.ima
```

```

Keyring
89159091 --alswrv 0 0 keyring: .ima
322584681 --als--v 0 0 \_ asymmetric: OS: TEST_SECURITY:
5d56a4ef2110df298945bbd33f6f8a9fa5a28004

```

Запустить утилиту ima-manage с ключом init:

```
/sbin/ima-manage init
```

Перезагрузить ЭВМ.

Запустить утилиту «ima-manage» с ключом «signfs» и указанием пути размещения секретного ключа:

```
/sbin/ima-manage signfs /root/key.pem
```

В файле /etc/fstab добавить к опциям монтирования файловой системы (defaults) опцию «iversion» (defaults,iversion):

```
UUID=ccb7f99f-5d40-428e-a277-be1d3cdaf2c4 / ext4 defaults,  
iversion 1 1
```

Запустить утилиту ima-manage с ключом «enforce»:

```
/sbin/ima-manage enforce
```

Дождаться завершения работы утилиты и предложения перезагрузки. Согласиться на перезагрузку ЭВМ.

Для использования сторонних приложений, не имеющих подписи разработчика, необходимо от имени администратора подписать файл:

```
evmctl ima_sign --key /root/key.pem файл
```

## 6.17 Блокирование файлов

В ряде случаев бывает необходимо защитить файлы, открытые кем-либо и используемые в текущий момент, от удаления любым другим пользователем, даже если он имеет на это права. Для поддержки этого функционала в РЕД ОС необходимо установить пакет fileprotect:

```
dnf install fileprotect
```

После установки пакета и перезагрузки ОС, блокируются попытки удаления файлов, если в момент обращения к файлу субъекта доступа (процесса) он используется другим субъектом доступа (процессом). Никаких дополнительных настроек не требуется.

## 6.18 Очистка памяти

В состав ОС входят утилиты «shred», «wipe», «nwipe» и набор консольных утилит Secure-Delete.

### 6.18.1 shred

Переписывает несколько раз указанные файлы для того, чтобы сделать более сложным восстановление даже с использованием очень дорогого оборудования.

Использование:

```
shred <КЛЮЧ>... <ФАЙЛ>...
```

Если <ФАЙЛ> задан как «-», измельчать стандартный вывод.  
Ключи утилиты shred описаны в таблице.

Ключ	Описание ключа
-f, --force	изменять права, разрешая запись, если необходимо.
-n, --iterations=N	переписать N раз вместо (3) по умолчанию.
--random-source=ФАЙЛ	получать случайные числа из <ФАЙЛА> (по умолчанию /dev/urandom).
-s, --size=N	очистить N байт (возможны суффиксы вида К, М, G).
-u	обрезать и удалять файл после перезаписи.
--remove [=КАК]	подобно «-u», но задаётся КАК удалять.
-v, --verbose	показывать ход выполнения.
-x, --exact	не округлять размеры файлов до следующего целого блока (по умолчанию для не простых файлов).
-z, --zero	перезаписать в конце нулями, чтобы скрыть измельчение.
--help	показать эту справку и выйти.
--version	показать информацию о версии и выйти.

Удаляет <ФАЙЛ(ы)>, если указан --remove (-u). По умолчанию файлы не удаляются, так как часто обрабатываются файлы-устройства вроде /dev/hda, а такие файлы не надо удалять.

Необязательным параметром КАК задаётся способ удаления каталога:

**unlink** – использовать стандартный вызов unlink.

**wipe** – также, сначала испортить байты имени.

**wipesync** – также, синхронизировать каждый испорченный байт на диске.  
Режим по умолчанию — «wipesync».

### 6.18.2 wipe

wipe — это небольшая программа для безопасного стирания файлов с магнитных носителей.

**Внимание!** Wipe надёжно работает только в магнитной памяти, следовательно, для твердотельных дисков (памяти) необходимо использовать другие методы. ■

Использование:

```
wipe <опции> <файлы>...
```

Основные опции утилиты `wipe` приведены в таблице.

Опция	Значение опции
-a	прервать при ошибке;
-b <buffer-size- lg2>	установить размер индивидуального буфера ввода/ вывода, указав его логарифм по основанию 2. Могут быть выделены до 30 этих буферов;
-c	делать <code>chmod()</code> на защищённых от записи файлах;
-D	следовать символическим ссылкам (конфликтует с «-r»);
-e	использовать точный размер файла: не округлять размер файла для стирания возможного мусора, остающегося на последнем блоке;
-f	форсировать, т. е. не спрашивать подтверждения;
-F	не пытаться стирать имена файлов;
-h	показать справку;
-i	информативный (вербальный) режим;
-k	сохранить файлы, т. е. не удалять их после перезаписи;
-l <длина>	установить длину стирания на <длина> байтов, где <длина> это целое число, за которым следует K (Kilo:1024), M (Mega:K <sup>2</sup> ) или G (Giga:K <sup>3</sup> );
-M (l r)	установить алгоритм PRNG для заполнения блоков (и порядка проходов): <ul style="list-style-type: none"> <li>• l – использовать вызов библиотеки <code>random()</code>;</li> <li>• a – использовать алгоритм шифрования <code>arcfour</code>.</li> </ul>
-o <сдвиг>	установить сдвиг очистки на <сдвиг>, где <сдвиг> имеет тот же формат, что и <длина>;
-P <проходы>	установить количество проходов для очистки имени файла. По умолчанию это 1;
-Q <количество>	установить количество проходов для быстрой очистки;
-q	быстрая очистка, менее безопасная, по умолчанию четыре случайных прохода;
-r	рекурсия по каталогам, по символическим ссылкам не будет переходов;
-R	установить устройство рандомизации (или команду сидов рандомизации -S c);

Опция	Значение опции
-S (r c p)	метод рандомизации сидов: <ul style="list-style-type: none"> <li>• r – считывать с устройства рандомизации (надёжно);</li> <li>• c – считывать из вывода команды рандомизации сидов;</li> <li>• p – использовать pid(), clock() и т.д. (самый слабый вариант).</li> </ul>
-s	тихий режим — подавлять весь вывод;
-T <попытки>	установить максимальное число попыток для свободного поиска имени файла (по умолчанию это 10);
-v	показать информацию о версии;
-Z	не пытаться стирать имя файла;
-X <число>	пропустить это число проходов (полезно для продолжения операции очистки);
-x <pass1,pass2, ...>	задать очередь проходов.

### 6.18.3 Secure-Delete

Secure-Delete – инструмент для стирания файлов, освобождения дискового пространства, swap'a и памяти. Этот набор консольных утилит предназначен для безвозвратного удаления данных и удаления остаточной информации. В своей работе использует Метод Гутмана.

В своём составе имеет набор из четырёх консольных утилит: srm, sfill, sswap, sdmem.

**Srm** - выполняет безопасную перезапись/переименование/удаление целевого файла(ов). При использовании ключа «-z» на последнем цикле удаления пишутся нули вместо случайных данных. По умолчанию включён безопасный режим (38 записей). Процесс безопасного удаления данных srm выглядит следующим образом:

- 1 проход с 0xff;
- 5 случайных проходов (если доступно, используется /dev/urandom для безопасного secure RNG);
- 27 проходов со специальными значениями, определёнными разработчиком;
- 5 случайных проходов (если доступно, используется /dev/urandom для безопасного RNG);
- переименование файлов на случайные значения;
- обрезка файлов.

В качестве дополнительной меры безопасности, файл открывается в режиме O\_SYNC и после каждого прохода делается вызов fsync(). srm записывает 32k блоков в целях быстрого действия, заполняя буферы дисковых кэшей, для принудительного их сброса и перезаписи старых данных, принадлежащих стираемому файлу, новыми данными.

Основные опции утилиты `Srm` приведены в таблице.

Опция	Значение опции
-d	игнорирует специальные файлы «.» и «..»;
-f	использует не безопасный, быстрый режим: без режимов <code>/dev/urandom</code> и <code>synchronize</code> ;
-l	снижение безопасности (двойное использование для полной не безопасности);
-r	использует рекурсивный режим для удаление всех подкаталогов;
-v	подробный вывода экран;
-z	затирание нулями на последнем шаге (вместо случайных чисел).

**Sfill** – аналогична предыдущей, только обрабатывает свободное место на диске, зачищая следы данных. `sfill` выполняет безопасную перезапись свободного места, занимаемого директорией, и всех свободных инодов заданной директории. По умолчанию безопасный режим (38 записей).

Процесс безопасного удаления данных `sfill` выглядит следующим образом:

- 1 проход с `0xff`;
- 5 случайных проходов (если доступно, используется `/dev/urandom` для безопасного secure RNG);
- 27 проходов со специальными значениями, определёнными разработчиком;
- 5 случайных проходов (если доступно, используется `/dev/urandom` для безопасного RNG).

После этого создаётся так много временных файлов, насколько это возможно, чтобы очистить свободное пространство индексных дескрипторов (`inode`). Когда больше невозможно создать временных файлов, они удаляются и `sfill` завершает свою работу.

Основные опции утилиты `Sfill` приведены в таблице.

Опция	Значение опции
-f	использует не безопасный, быстрый режим: без режимов <code>/dev/urandom</code> и <code>synchronize</code> ;
-l	снижение безопасности (двойное использование для полной не безопасности);
-r	использует рекурсивный режим для удаление всех подкаталогов;
-v	подробный вывода экран;
-z	затирание нулями на последнем шаге (вместо случайных чисел).

**Sswap** – зачищает раздел подкачки /swap, если он присутствует в системе. Перед использованием необходимо отключить swap. По умолчанию безопасный режим (38 записей).

Процесс безопасного удаления данных Sswap выглядит следующим образом:

- 1 проход с 0xff;
- 5 случайных проходов (если доступно, используется /dev/urandom для безопасного secure RNG);
- 27 проходов со специальными значениями, определёнными разработчиком;
- 5 случайных проходов (если доступно, используется /dev/urandom для безопасного RNG).

Основные опции утилиты Sswap приведены в таблице.

Опция	Значение опции
-f	использует не безопасный, быстрый режим: без режимов /dev/urandom и synchronize;
-l	снижение безопасности (двойное использование для полной не безопасности);
-r	использует рекурсивный режим для удаление всех подкаталогов;
-v	подробный вывода экран;
-z	затираание нулями на последнем шаге (вместо случайных чисел).

**Sdmem** – уничтожает следы данных в оперативной памяти. sdmem выполняет безопасную перезапись оперативной памяти (RAM), поскольку содержимое памяти может быть восстановлено даже после отключения. По умолчанию безопасный режим (38 записей).

Основные опции утилиты Sdmem приведены в таблице.

Опция	Значение опции
-f	использует не безопасный, быстрый режим: без режима /dev/urandom;
-l	снижение безопасности (двойное использование для полной не безопасности);
-v	подробный вывода экран.

## 6.19 Экспорт данных пользователя

Для экспортирования данных используется утилита sr.

sr — команда, предназначенная для копирования файлов из одного в другие каталоги (возможно, с другой файловой системой). Исходный файл остаётся неизменным, имя созданного файла может быть таким же, как у исходного, или измениться.

Чтобы скопировать файл:

```
ср [ -f ] [ -h ] [ -i ] [ -p ] [ -- ] <исходный_файл>
<целевой_файл>
```

Чтобы скопировать файл или файлы в другой каталог:

```
ср [-R] [-H | -L | -P] [-f | -i] [-pv]
<исходный_файл> ... <целевой_каталог>
```

Чтобы скопировать каталог в другой каталог (должен быть использован флаг -r или -R):

```
ср [ -f ] [ -h ] [ -i ] [ -p ] [ -- ] { -r | -R }
<исходный_каталог> ... <целевой_каталог>
```

Чтобы скопировать каталог /media/fff1787/share1/load/ в каталог /media/beacbe58/, с выводом имени копируемого файла, автоматическим пропуском существующих файлов, рекурсивно для вложенных каталогов.

```
ср -invR /media/fff1787/share1/load/ /media/beacbe58/
```

Опции команды описаны в таблице.

Опция	Значение опции
-R, -r, --recursive (recursive)	копировать каталоги рекурсивно (то есть все подкаталоги и все файлы в подкаталогах);
-f (force)	разрешает удаление целевого файла, в который производится копирование, если он не может быть открыт для записи;
-H	используйте этот ключ, чтобы копировать символические ссылки. По умолчанию команда переходит по символическим ссылкам и копирует файлы, на которые те указывают;
-i (interactive)	команда будет запрашивать, следует ли перезаписывать конечный файл, имя которого совпадает с именем исходного, то есть если в параметре <целевой_каталог> или <целевой_файл> встречается такое же имя файла, какое было задано в параметре <исходный_файл> или <исходный_каталог>, то запрашивается подтверждение. Для того, чтобы перезаписать файл, следует ввести «у» или его эквивалент для данной локали. Ввод любого другого символа приведёт к отмене перезаписи данного файла;
-n, --no-clobber	не перезаписывать существующий файл (отменяет предыдущий параметр -i);
-v, --verbose	выводит имя каждого файла перед его копированием;

Опция	Значение опции
-p (preserve)	повторяет следующие свойства исходного файла или каталога у целевого файла или каталога: <ul style="list-style-type: none"> <li>• время последнего изменения и последнего доступа;</li> <li>• идентификатор пользователя и группы;</li> <li>• права доступа и биты SUID и SGID.</li> </ul>

## 6.20 Резервирование данных

В состав дистрибутива ОС входит утилита резервного копирования `rsync`. `rsync` (англ. Remote Synchronization) — программа, которая выполняет синхронизацию файлов и каталогов в двух местах с минимизированием трафика, используя сжатие данных при необходимости. Важным отличием `rsync` от многих других программ/протоколов является то, что зеркалирование осуществляется одним потоком в каждом направлении (а не по одному или несколько потоков на каждый файл). `rsync` может копировать или отображать содержимое каталога и копировать файлы, опционально используя сжатие и рекурсию.

`rsyncd` — демон, реализующий протокол `rsync`. По умолчанию использует TCP-порт 873.

Базовый синтаксис:

```
rsync <опции> <источник> <место_назначения>
```

Наиболее полезные опции `rsync` приведены в таблице:

Опция	Значение опции
-v	подробный режим;
-r	копировать данные рекурсивно (но без сохранения информации о времени изменения файлов и правах доступа);
-a	режим архивирования, позволяет копировать данные рекурсивно с сохранением симлинков, правах доступа на файлы/-каталоги и другую информацию);
-z	сжатие данные;
-h	вывод данных в human-readable формате.

## 6.21 Лимиты ресурсов

В состав дистрибутива входит утилита `ulimit`, позволяющая управлять аппаратными ресурсами. `limits.conf` - это конфигурационный файл для `ram_limits.so` модуля. Он определяет `ulimit` лимиты для пользователей и групп. Конфигурация по умолчанию находится в `/etc/security/limits.conf`. Также присутствует возможность добавлять отдельные настройки для приложений в `/etc/security/limits.d`.

В данном примере для группы `<limit_users>` введены жёсткие ограничения.

Формат таков:

```
<группа>/<пользователь> <лимит>(жёсткий/мягкий) <параметр>  
<значение>
```

Описание параметров:

**core** – размер core-файлов (KB);

**data** – максимальный размер данных (KB);

**fsize** – максимальный размер файла (KB);

**memlock** – максимальное заблокированное адресное пространство (KB);

**nofile** – максимальное количество открытых файлов;

**rss** – максимальный размер памяти для резидент-программ (KB);

**stack** – максимальный размер стэка (KB);

**cpu** – максимальное процессорное время (MIN);

**proc** – максимальное количество процессов;

**as** – ограничение адресного пространства (KB);

**maxlogins** – максимальное число одновременных регистраций в системе;

**maxsyslogins** – максимальное количество учётных записей;

**priority** – приоритет запущенных процессов;

**locks** – максимальное количество блокируемых файлов пользователем;

**sigpending** – максимальное количество сигналов, которые можно передать процессу;

**msgqueue** – максимальный размер памяти для очереди POSIX сообщений (bytes);

**nice** – максимальный приоритет, который можно выставить: [-20, 19];

**rtprio** – максимальный приоритет времени выполнения;

**chroot** – изменить директорию root'a (Debian-specific).

Вместо групп/юзера можно использовать групповой символ «\*» (для всех) и групповой символ «%» для wildcard'а групп.

Параметры вступают в силу сразу после перелога пользователя. Что бы посмотреть какие действуют ограничения, используйте команду ulimit:

```
ulimit -aH
```

## 6.22 Монтирование файловых систем

**mount** — утилита командной строки для монтирования файловых систем.

Использование:

```
mount /dev/cdrom /mnt/cdrom
```

Устройство /dev/cdrom монтируется в каталог /mnt/cdrom, если он существует. Начиная от момента монтирования и пока пользователь не отмонтирует файловую систему (или туда не будет смонтировано что-то иное), в каталоге /mnt/cdrom будет содержаться дерево каталогов устройства /dev/cdrom; те файлы и подкаталоги, которые раньше находились в /mnt/cdrom, сохранятся, но будут недоступны до размонтирования устройства /dev/cdrom.

Для размонтирования достаточно указать точку монтирования или имя устройства.

```
umount /dev/cdrom
```

В случае необходимости, при выполнении команды `mount`, можно указать дополнительные параметры монтирования.

```
-t <Тип файловой системы>
```

Обычно при монтировании определяется автоматически или берётся из файла конфигурации. Но в отдельных случаях нужно указывать тип файловой системы явно. Например, при монтировании DVD-диска.

```
mount /dev/cdrom /mnt/dvd -t udf
```

Если неправильно указать тип файловой системы, то команда `mount` выдаст сообщение об ошибке:

```
mount: wrong fs type, bad option, bad superblock on /dev/cdrom,
missing codepage or other error
In some cases useful info is found in syslog - try
dmesg | tail or so
```

и посоветует посмотреть в конец файла системных сообщений.

```
Unable to identify CD-ROM format.
```

В случае успешного монтирования обычно сообщается, что компакт-диск монтируется (по умолчанию) в режиме «только для чтения».

```
mount: block device /dev/cdrom is write-protected, mounting
read-only
```

```
-o <Атрибуты доступа>
```

- Доступ «только для чтения» (`ro`) или на «чтение и запись» (`rw`);
- Разрешение или запрещение запуска программ (`noexec`).

При запуске команды `mount` без параметров выводится список смонтированных файловых систем:

```
/dev/md/5 on / type reiserfs (rw,noatime)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec)
udev on /dev type tmpfs (rw,nosuid)
```

Чтобы облегчить процедуру монтирования, можно внести в файл конфигурации `/etc/fstab` соответствующие строки. Примерное содержимое для этого файла:

```
# <fs> <mountpoint> <type> <opts> <dump/pass>
# NOTE: If your BOOT partition is ReiserFS, add the notail option
to opts.
#/dev/BOOT /boot ext3 noauto,noatime 1 2
/dev/sda5 / reiserfs noatime 0 1
/dev/sda1 none swap sw 0 0
# NOTE: The next line is critical for boot!
proc /proc proc defaults 0 0
```

В дальнейшем можно будет указывать в команде `mount` только имя устройства или точку монтирования — все дополнительные параметры будут браться из файла конфигурации.

Другое назначения файла конфигурации — автоматическое монтирование файловых систем при загрузке системы. Если не требуется монтировать определённые файловые системы, то для них в файле конфигурации нужно указать параметр `noauto`.

### 6.23 Принудительное завершение сеанса пользователя

Для отслеживания времени бездействия пользователя и завершения сеанса используется скрипт `/usr/bin/gui-kick`. Сценарий использует системную переменную `«xprintidle»`, которая показывает время бездействия пользователя в графическом сеансе в миллисекундах. Есть две границы «предупреждение» и «завершение сеанса». После превышения границы «предупреждение», пользователю через службу `notify-send` формируется предупреждение о скором завершении сеанса и выводится в графическом сеансе соответствующее сообщение. После превышения второго заданного в сценарии максимального значения времени бездействия, сценарий принудительно завершает работу графического сеанса.

Для отслеживания бездействия пользователя необходимо добавить новое задание в демон `cron`:

```
echo "* * * * * root /usr/bin/gui-kick" >> /etc/crontab
```

Установить интервал бездействия пользователя (в секундах) можно, присваивая новое значение переменной `TIMEOUT` в скрипте `/usr/bin/gui-kick`.

За 60 секунд до завершения сессии выводится системное уведомление с предупреждением о том, что по истечении 1 минуты завершится сессия, и чтобы этого избежать, необходимо предпринять какие-либо действия. Если в течение следующих 60 секунд пользователь по-прежнему не предпринял никаких действий, сессия пользователя завершается принудительно.

# Управление пользователями

## 7. Управление пользователями

### 7.1 Общая информация

РЕД ОС – многопользовательская операционная система. Также имеются группы пользователей, основное предназначение которых - облегчить управление большим количеством пользователей, а также более точно распределить права доступа к различным объектам системы. Пользователи и группы внутри системы обозначаются цифровыми идентификаторами - UID и GID, соответственно.

Пользователь может входить в одну или несколько групп. По умолчанию он входит в группу, совпадающую с его именем. Чтобы узнать, в какие ещё группы входит пользователь, введите команду `id`, вывод ее может быть примерно следующим:

```
uid=500(test) gid=500(test) группы=500(test),16(rpm)
```

Такая запись означает, что пользователь `test` (цифровой идентификатор 500) входит в группы `test` и `rpm`. Разные группы могут иметь разный уровень доступа к тем или иным каталогам; чем в большее количество групп входит пользователь, тем больше прав он имеет в системе.

**Внимание!** В связи с тем, что в дистрибутивах РЕД ОС большинство привилегированных системных утилит имеют не SUID-, а SGID-бит, будьте предельно внимательны и осторожны в переназначении групповых прав на системные каталоги. ■

## 7.2 Утилита passwd

Утилита `passwd` поддерживает традиционные опции «`passwd`» и утилиту «`shadow`».

Синтаксис:

```
passwd <ОПЦИЯ...> <ИМЯ_ПОЛЬЗОВАТЕЛЯ>
```

Основные опции утилиты `passwd` приведены в таблице.

Опция	Значение опции
<code>-d</code> , <code>--delete</code>	Удалить пароль для указанной записи.
<code>-f</code> , <code>--force</code>	Форсировать операцию.
<code>-k</code> , <code>--keep-tokens</code>	Сохранить не устаревшие пароли.
<code>-l</code> , <code>--lock</code>	Блокировать указанную запись.
<code>--stdin</code>	Прочитать новые пароли из стандартного ввода.
<code>-S</code> , <code>--status</code>	Дать отчёт о статусе пароля в указанной записи.
<code>-u</code> , <code>--unlock</code>	Разблокировать указанную запись.
<code>-?</code> , <code>--help</code>	Показать справку и выйти.
<code>--usage</code>	Дать короткую справку по использованию.
<code>-V</code> , <code>--version</code>	Показать версию программы и выйти.

При успешном завершении «`passwd`» заканчивает работу с кодом выхода «0». Код выхода «1» означает, что произошла ошибка. Текстовое описание ошибки выводится на стандартный поток ошибок.

## 7.3 Добавления нового пользователя

Для добавления нового пользователя используйте команды «`useradd`» и «`passwd`». В примере в качестве первоначально введённого пароля указана последовательность символов «123», затем введён надёжный пароль:

```
useradd test1  
passwd test1
```

Смена пароля для пользователя `test1`:

```

Новый пароль:
НЕУДАЧНЫЙ ПАРОЛЬ: СЛИШКОМ короткий
НЕУДАЧНЫЙ ПАРОЛЬ: СЛИШКОМ простой
Повторите ввод нового пароля:
passwd: все токены проверки подлинности успешно обновлены.

```

В результате описанных действий в системе появился пользователь `test1` с некоторым паролем. Если пароль оказался слишком слабым с точки зрения системы, она об этом предупредит (как в примере выше). Пользователь в дальнейшем может поменять свой пароль при помощи команды «`passwd -`», но если он попытается поставить слабый пароль, система откажет ему (в отличие от `root`) в изменении.

В дистрибутивах ОС для проверки паролей на слабость используется модуль PAM «`passwdqc`».

Программа «`useradd`» имеет множество параметров, которые позволяют менять ее поведение по умолчанию. Например, можно принудительно указать, какой будет UID или какой группе будет принадлежать пользователь.

Синтаксис:

```

useradd [-u <идентификатор> [-o] [-i]] [-g <группа>] [-G <группа>
[[,<группа>]...]] [-d <каталог>] [-s <shell>] [-c <комментарий>]
[-m [-k <skel_dir>]] [-f <inactive>] [-e <expire>] [-p <passgen>]
[-a <событие>[,...]] <рег_имя>

```

Основные опции команды `useradd` приведены в таблице.

Опция	Значение опции
<code>-u</code> <идентификатор>	Идентификационный номер пользователя (UID). Этот номер должен быть неотрицательным целым числом, не превосходящим <code>MAXUID</code> , определённый в <code>sys/param.h</code> . По умолчанию используется следующий доступный (уникальный) не устаревший UID, больший 99. Эта опция игнорируется, если новое регистрационное имя будет администрироваться сетевой информационной службой (NIS).
<code>-o</code>	Эта опция позволяет сдублировать UID (сделать его не уникальным). Поскольку защита системы в целом, а также целостность контрольного журнала ( <code>audit trail</code> ) и учётной информации ( <code>accounting information</code> ) в частности, зависит от однозначного соответствия каждого UID определённому лицу, использовать эту опцию не рекомендуется (чтобы обеспечить учёт действий пользователей).
<code>-i</code>	Позволяет использовать устаревший идентификатор UID.

Опция	Значение опции
-g <группа>	Целочисленный идентификатор или символьное имя существующей группы. Эта опция задаёт основную группу (primary group) для нового пользователя. По умолчанию используется стандартная группа, указанная в файле /etc/default/useradd. Эта опция игнорируется, если новое регистрационное имя будет администрироваться сетевой информационной службой (NIS).
-G <группа> [[, <группа>] ...]	Один или несколько элементов в списке через запятую, каждый из которых представляет собой целочисленный идентификатор или символьное имя существующей группы. Этот список определяет принадлежность к дополнительным группам (supplementary group membership) для пользователя. Повторения игнорируются. Количество элементов в списке не должно превосходить <NGROUPS_MAX> - 1, поскольку общее количество дополнительных групп для пользователя плюс основная группа не должно превосходить <NGROUPS_MAX>. Эта опция игнорируется, если новое регистрационное имя будет администрироваться сетевой информационной службой (NIS).
-d <каталог>	Начальный каталог (home directory) нового пользователя. Длина этого поля не должна превосходить 256 символов. По умолчанию используется HOMEDIR/<рег_имя>, где HOMEDIR - базовый каталог для начальных каталогов новых пользователей, а <рег_имя> - регистрационное имя нового пользователя.
-s <shell>	Полный путь к программе, используемой в качестве начального командного интерпретатора для пользователя сразу после регистрации. Длина этого поля не должна превосходить 256 символов. По умолчанию это поле - пустое, что заставляет систему использовать стандартный командный интерпретатор /usr/bin/sh. В качестве значения shell должен быть указан существующий выполняемый файл.
-c <комментарий>	Любая текстовая строка. Обычно, это краткое описание регистрационного имени и используется сейчас для указания фамилии и имени реального пользователя. Эта информация хранится в записи пользователя в файле /etc/passwd. Длина этого поля не должна превосходить 128 символов.
-m	Создаёт начальный каталог нового пользователя, если он ещё не существует. Если каталог уже существует, добавляемый пользователь должен иметь права на доступ к указанному каталогу.

Опция	Значение опции
-k <skel_dir>	Копирует содержимое каталога <skel_dir> в начальный каталог нового пользователя, вместо содержимого стандартного «скелетного» каталога /etc/skel. Каталог <skel_dir> должен существовать. Стандартный «скелетный» каталог содержит стандартные файлы, определяющие среду работы пользователя. Заданный администратором каталог <skel_dir> может содержать аналогичные файлы и каталоги, созданные для определённой цели.
-f <inactive>	Максимально допустимое количество дней между использованиями регистрационного имени, когда это имя ещё не объявляется недействительным. Обычно в качестве значений используются положительные целые числа.
-e <expire>	Дата, начиная с которой регистрационное имя больше нельзя будет использовать; после этой даты никакой пользователь не сможет получить доступ под этим регистрационным именем. (Эта опция удобна при создании временных регистрационных имён.) Вводить значение аргумента expire (представляющего собой дату) можно в любом формате (кроме Julian date). Например, можно ввести 10/6/99 или October 6, 1999.
-p <passgen>	Указывает, что поле FLAG в файле /etc/shadow должно быть установлено в указанное значение. К этому полю обращается команда «passwd», чтобы определить, действует ли для данного пользователя генератор паролей. Если опция «-p» явно не задана, проверяется запись <FORCED_PASS> в файле /etc/default/useradd, чтобы определить значение для соответствующего поля в /etc/shadow. Если записи <FORCED_PASS> нет в /etc/default/useradd, в соответствующем поле записи в /etc/shadow значения не будет. Если значение <FORCED_PASS> равно 1, запись в /etc/shadow получает значение 1. Если значение passgen не пустое и не является печатным символом ASCII, выдаётся диагностическое сообщение.
-a <событие>	Список типов или классов событий через запятую, образующих маску аудита (audit mask) для пользователя. Сразу после установки системы стандартной маски аудита для пользователя нет, но ее можно задать в файле /etc/default/useradd с помощью команды defadm. Эту опцию можно использовать, только если установлены утилиты аудита (Auditing Utilities).

Опция	Значение опции
<рег_имя>	Строка печатных символов, задающая регистрационное имя для нового пользователя. В имени пользователя допускается латиница нижнего регистра, цифры, подчёркивание и дефис (короткое тире). Первым символом должна быть или буква или подчёркивание. Длина строки имени пользователя до 32-х символов.

## 7.4 Модификация уже имеющихся пользовательских записей

Для модификации уже имеющихся пользовательских записей применяется утилита `usermod`:

```
usermod -G audio,rpm,test1 test1
```

Такая команда изменит список групп, в которые входит пользователь `test1` – теперь это `audio, rpm, test1`.

```
usermod -l test2 test1
```

Будет произведена смена имени пользователя с `test1` на `test2`.

Команды

```
usermod -L test2
```

и

```
usermod -U test2
```

соответственно временно блокируют возможность входа в систему пользователю `test2` и возвращают все на свои места.

Изменения вступят в силу только при следующем входе пользователя в систему.

При неинтерактивной смене или задании паролей для целой группы пользователей используйте утилиту «`chpasswd`». На стандартный вход ей следует подавать список, каждая строка которого будет выглядеть как:

```
<имя>:<пароль>
```

## 7.5 Удаление пользователей

Для удаления пользователей используйте `userdel`.

Команда

```
userdel test2
```

удалит пользователя `test2` из системы. Если будет дополнительно задан параметр «`-d`», то будет уничтожен и домашний каталог пользователя. Нельзя удалить пользователя, если в данный момент он ещё работает в системе.

Утилиты «vigr» и «vipw» используются для ручного редактирования файлов /etc/passwd и /etc/group, в которых хранятся основные записи о пользователях и группах в системе.

Не рекомендуется создавать пользователей с правами сверх необходимых. Предпочтительнее создать серию новых групп и включить в них требуемого пользователя. А для данных групп установить соответствующие права на объектах файловой системы (утилиты «chmod» и «chown»).

## 7.6 Пароли пользователей

/etc/passwd — файл, содержащий в текстовом формате список пользовательских учётных записей (аккаунтов).

Является первым и основным источником информации о правах пользователя операционной системы.

Принцип:

```
login : password : UID : GID : GECOS : home : shell
```

Каждая строка файла описывает одного пользователя и содержит семь полей, разделённых двоеточиями:

- регистрационное имя или логин;
- хеш пароля;
- идентификатор пользователя;
- идентификатор группы по умолчанию;
- информационное поле GECOS;
- начальный (он же домашний) каталог;
- регистрационная оболочка, или shell.

Основным назначением /etc/passwd является сопоставление логина и идентификатора пользователя (UID). Изначально поле пароля содержало хеш пароля и использовалось для аутентификации. Однако, в связи с ростом вычислительных мощностей процессоров появилась серьёзная угроза применения простого перебора для взлома пароля. Поэтому все пароли были перенесены в специальные файлы, такие как /etc/shadow. Эти файлы недоступны для чтения обычным пользователям. Такой подход называется механизмом скрытых паролей.

Регистрационные имена должны быть уникальными и представлять собой строки не длиннее 32 символов (любые, кроме двоеточия и символа новой строки). По сути, имя пользователя — это его короткий и легко запоминаемый псевдоним, который используется при входе в систему и часто включается в адреса электронной почты.

Идентификатор пользователя — это число от 0 до 232-1. Пользователь с идентификатором «0» (обычно root) называется суперпользователем и имеет право на выполнение любых операций в системе. Принято соглашение о выделении «специальным» пользователям (bin, daemon), назначение которых — только запуск определённых программ, маленьких идентификаторов (меньше 100).

Пользователь может принадлежать к одной или нескольким группам, которые используются для задания прав более чем одного пользователя на тот или иной файл.

Список групп с их участниками задаётся в `/etc/group`. В файле же `/etc/passwd` указывается идентификатор группы по умолчанию.

Всем файлам, созданным пользователем после регистрации в системе, будет автоматически присвоен этот номер группы (исключение — если для каталога, в котором создаётся файл, установлен в правах бит SGID, то будет присвоена такая же группа, как у самого каталога).

`/etc/group` содержит записи обо всех группах в системе. Каждая его строка содержит:

- символьное имя группы;
- пароль группы — устаревшее поле, сейчас не используется. В нём обычно стоит «x»;
- идентификатор группы, или GID;
- список имён участников, разделённых запятыми.

Пример записи:

```
bin:x:1:root,bin,daemon
```

Здесь сообщается, что группа `bin` имеет `GID=1`, а входят в неё пользователи `root`, `bin` и `daemon`.

Поле GECOS хранит вспомогательную информацию о пользователе (номер телефона, адрес, полное имя и так далее). Оно не имеет чётко определённого синтаксиса.

Тем не менее, демон «`fingerd`» предполагает, что в нём содержатся следующие элементы, разделённые запятыми:

- полное имя;
- адрес офиса или домашний адрес;
- рабочий телефон;
- домашний телефон.

С помощью утилиты «`chfn`» можно изменять эту информацию, а с помощью «`finger`» — узнать, например, полное имя любого пользователя в системе (или даже на другом компьютере сети).

Пример строки с заполненным полем GECOS:

```
tester:x:210:8:Edward Chernenko,Marx Street 10,4554391,5454221:  
/home/ed:/bin/bash
```

После входа в систему пользователь оказывается в своём домашнем каталоге. Исторически сложилось так, что домашний каталог пользователя `root` называется `/root`, а остальные имеют вид `/home/<имя_пользователя>`.

Если на момент входа в систему домашний каталог отсутствует, то система выдаёт сообщение об ошибке и отказывается допустить пользователя к командной строке. Это можно изменить посредством установки параметра `<DEFAULT_HOME>` в файле `/etc/login.defs` в значение «no».

Следует отметить, что при использовании графического интерфейса пользователь не увидит предупреждения или сообщения об ошибке, но просто будет выведен из системы безо всяких объяснений (так как оконный менеджер не сможет выполнить запись в нужный каталог, такой как `~/gnome`).

В поле регистрационной оболочки задаётся shell, то есть интерпретатор командной строки. Здесь может быть указана любая программа, и пользователь может сам выбирать для себя наиболее подходящую при помощи команды «chsh». Тем не менее некоторые системы в целях безопасности требуют, чтобы суперпользователь явно разрешил использовать приложение в качестве интерпретатора командной строки. Для этого используется специальный файл /etc/shells, содержащий список «допустимых» оболочек.

vi<sub>rw</sub> - запускает текстовый редактор, указанный в переменной среды EDITOR (или редактор по умолчанию, обычно vi), загружая в него копию файла /etc/passwd. После закрытия редактора переносит временную копию в сам файл. Не позволяет двум пользователям выполнять редактирование одновременно.

В файле /etc/shadow хранятся хеши паролей всех пользователей в системе. Процессы суперпользователя могут читать его напрямую, а для остальных создана специальная библиотека PAM. Она позволяет непривилегированным приложениям спрашивать у неё, правильный ли пароль ввёл пользователь, и получать ответ. Библиотека PAM, как правило, действует с привилегиями вызвавшего процесса. Таким образом, хеш не попадает «в чужие руки».

Пароль шифруется с MD5-хешированием или blowfish-хешированием (bcrypt), MD5-хеши всегда записываются после префикса «\$1\$».

Перед хешированием к паролю добавляются случайные символы — «salt» (соль, от англ. add salt to something — сделать что-либо более интересным; в русскоязычных источниках иногда используется термин «затравка»). Salt также приписывается к началу полученного хеша. Благодаря salt нельзя при простом просмотре файла обнаружить пользователей с одинаковыми паролями.

Кроме имени (первое поле каждой строки) и хеша (второе поле) в файле /etc/shadow также хранятся:

- дата последнего изменения пароля;
- через сколько дней можно будет поменять пароль;
- через сколько дней пароль устареет;
- за сколько дней до того, как пароль устареет, начать напоминать о необходимости смены пароля;
- через сколько дней после того, как пароль устареет, заблокировать учётную запись пользователя;
- дата, при достижении которой учётная запись блокируется;
- зарезервированное поле.

Даты обозначаются как число дней с 1 января 1970 года.

ОС поддерживает управление качеством используемых паролей. Рассмотрим настройку различных параметров используемых паролей.

**Время действия пароля** (по истечении указанного времени пользователь должен будет сменить пароль).

Необходимо в конфигурационном файле /etc/login.defs изменить параметр <PASS\_MAX\_DAYS>

Обратите внимание, что данное требование будет работать только для вновь создаваемых пользователей, для уже существующих нужно использовать команду:

```
chage -M <days> <user>
```

Если пользователю необходимо выдавать предупреждение за несколько дней до окончания срока действия пароля, необходимо использовать параметр `<PASS_WARN_AGE>`

#### **Предел числа используемых ранее паролей.**

Изменить в файле `/etc/pam.d/system-auth` следующий параметр:

```
password sufficient pam_unix.so sha512 shadow nullok  
try_first_pass use_authok remember=5
```

#### **Установить минимальную длину пароля.**

Изменить в конфигурационном файле `/etc/security/pwquality.conf` параметр:

```
minlen= -8
```

#### **Установить минимальное число строчных букв в новом пароле.**

Изменить в конфигурационном файле `/etc/security/pwquality.conf` параметр:

```
lcredit = -1
```

#### **Установить минимальное число заглавных букв в новом пароле.**

Изменить в конфигурационном файле `/etc/security/pwquality.conf` параметр:

```
ucredit = -1
```

#### **Установить минимальное число цифр в новом пароле.**

изменить в конфигурационном файле `/etc/security/pwquality.conf` параметр:

```
dccredit = -1
```

#### **Установить минимальное число спецсимволов в новом пароле.**

Изменить в конфигурационном файле `/etc/security/pwquality.conf` параметр:

```
ocredit = -1
```

Для изменения срока действия пароля необходимо использовать утилиту «chage».

Синтаксис:

```
chage [-m <mindays>] [-M <maxdays>] [-d <lastday>] [-I <inactive>]  
[-E <expiredate>] [-W <warndays>] <user>  
chage -l <user>
```

chage изменяет количество дней между сменой пароля и датой последнего изменения пароля. Информация используется системой для определения времени, когда пользователь должен сменить свой пароль. Команда chage разрешена только для суперпользователя, за исключением использования ее с параметром «-l», который позволяет непривилегированным пользователям определить время, когда истекает их пароль или учётная запись.

С параметром «-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.

С параметром «-M» изменяется значение `<maxdays>` на максимальное число дней, в течение которых пароль ещё действителен. Когда сумма `<maxdays>` и `<lastday>` меньше, чем текущий день, у пользователя будет запрошен новый пароль до начала работы в системе. Эта операция может предваряться предупреждением (параметр «-W»).

С параметром «-d» изменяется значение `<lastday>` на день, когда был изменён пароль последний раз (число дней с 1 января 1970). Дата также может быть указана в формате `<ГГГГ-ММ-ДД>` (или формат, используемый в вашем регионе).

Параметр «-E» используется для задания даты, с которой учётная запись пользователя станет недоступной. Параметр `<expiredate>` есть число дней с 1 января 1970. Дата также может быть указана в формате `<ГГГГ-ММ-ДД>` (или формат, используемый в вашем регионе). Пользователь, чья учётная запись была заблокирована, должен сообщить об этом администратору для дальнейшей работы в системе.

Параметр «-I» используется для задания количества дней «неактивности», то есть дней, когда пользователь вообще не входил в систему, после которых его учётная запись будет заблокирована. Пользователь, чья учётная запись была заблокирована, должен сообщить об этом администратору для дальнейшей работы в системе. Параметр `<inactive>` есть количество «неактивных» дней. Значение «0» отключает этот режим.

Параметр «-W» используется для задания числа дней, с которых пользователю начнёт выводиться предупреждение об истечении срока действия его пароля и необходимости его изменения. Параметр `<warndays>` есть число дней до истечения срока действия пароля, с которых пользователю будет выдаваться предупреждение.

Все вышеперечисленные значения хранятся в виде дней, если используется система теневого паролей, но если используется системы обычных паролей, то значения преобразуются в недели. Из-за этого преобразования могут происходить ошибки округления.

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 [ ].

## 7.7 Роли пользователей

В ОС пользователи по умолчанию сопоставляются SELinux-пользователю `<unconfined_u>`. SELinux-пользователь `<unconfined_u>`, в свою очередь, сопоставлен ролям `<unconfined_r>` и `<system_r>`.

Обе роли `<unconfined_r>` и `<system_r>` сопоставляются доменам безопасности SELinux. Домены безопасности SELinux - это определённые окружения безопасности для процессов.

Неограниченный домен безопасности – `<unconfined_t>` – зарезервированное окружение для процессов, которые в значительной степени освобождены от ограничений SELinux. Роль `<system_r>` сопоставляется доменам безопасности для системных процессов.

SELinux-пользователь `<unconfined_u>` имеет доступ к роли `<system_r>`, чтобы иметь возможность запускать системные процессы в своих доменах безопасности. SELinux-пользователь `<unconfined_u>` работает в домене безопасности `<unconfined_t>` через роль `<unconfined_r>`, которой он сопоставлен.

Команда «semanage» позволяет добавлять, изменять и удалять сопоставления между ОС- и SELinux-пользователями, так же как и другие настройки, касающиеся управления SELinux.

Чтобы с помощью команды «semanage» посмотреть какому SELinux-пользователю по умолчанию сопоставлены пользователи ОС наберите:

```
semanage login -l | grep default
```

В примере выше пользователи по умолчанию сопоставлены SELinux-пользователю `<unconfined_u>`.

Чтобы изменить это и сопоставить пользователей по умолчанию ограниченному SELinux-пользователю с именем `<user_u>` просто наберите:

```
semanage login -m -s user_u "__default__"
```

В результате все новые пользователи будут по умолчанию сопоставляться ограниченному SELinux-пользователю `<user_u>`.

Вы можете переопределить данное сопоставление при добавлении пользователей командой «useradd» используя опцию «-Z». Эта опция определяет какому SELinux-пользователю должен быть сопоставлен пользователь ОС.

Например наберите:

```
useradd -Z guest_u joe
```

В результате будет создан новый пользователь с именем joe, который будет сопоставлен SELinux-пользователю `<guest_u>`, вместо определённого по умолчанию SELinux-пользователя.

Также для изменения сопоставления между пользователем и SELinux-пользователем может быть использована команда «usermod» с опцией «-Z».

Существует несколько предопределённых профилей SELinux-пользователей. Список данных профилей можно вывести командой «semanage», наберите:

```
semanage user -l
```

SELinux-пользователь `<unconfined_u>` это среда, в которой по умолчанию работают все пользователи. Этот пользователь в значительной степени освобождён от ограничений, накладываемых SELinux. Если Вы хотите повысить безопасность вашей системы, тогда не следует сопоставлять реальных пользователей, не пользователя root, SELinux-пользователю `<unconfined_u>`.

Вход пользователя `root` должен быть запрещён. `Root` должен иметь возможность войти с терминала только в случае крайней необходимости. Чтобы повысить безопасность использования `root` можно сопоставить пользователя `root` SELinux-пользователю `<sysadm_u>`.

Ролевой доступ SELinux используется для обеспечения возможности назначения нескольких ограниченных окружений SELinux одному SELinux-пользователю.

В SELinux роли пользователя (User Roles) - это домены пользователя или пользовательские домены (User Domains). Когда упоминаются роли, часто имеется в виду дополнительный (secondary) пользовательский домен пользователя SELinux. Часто роли, предназначенные для использования в качестве дополнительных доменов пользователя, отличаются от основных (primary) доменов. Это объясняется тем, что пользователи ОС фактически не используют для входа в систему роли, созданные как дополнительные домены пользователя. Вместо этого пользователи Linux, используя команду «`sudo`» или комбинацию команд «`su`» и «`newrole`», осуществляют переключение домена или доменный переход (Domain Transition) к их дополнительной роли.

#### Роль администратора - `Sysadm`.

Пример роли, предназначенной для использования в качестве основного домена пользователя. SELinux пользователь `<sysadm_u>` сопоставлен роли `<sysadm_r>`. Это сопоставление можно увидеть, выполнив команду:

```
semanage user -l | grep sysadm_u
```

По умолчанию пользователи ОС, сопоставленные пользователю SELinux `<sysadm_u>`, работают с ролью `<sysadm_r>`. В этом случае `<sysadm_r>` — это основной домен пользователя.

SELinux пользователь `<staff_u>` также сопоставлен роли `<sysadm_r>`. Основным пользовательским доменом пользователя SELinux `<staff_u>` является (роль) `<staff_r>`. Контексты по умолчанию, определённые в `/etc/selinux/targeted/contexts/users/staff_u`, определяют с какими пользовательскими доменами пользователи будут подключаться по умолчанию и с какими пользовательскими доменами пользователи могут войти, указав домен пользователя при входе.

По умолчанию SELinux пользователь `<staff_u>` входит в систему в домен пользователя `<staff_t>`. Роль `<sysadm_r>`, предназначенная для использования в качестве основного домена пользователя, может быть использована при входе, например, следующим образом:

```
ssh joe/sysadm_r@localhost.localdomain.tld
```

Также роль `<sysadm_r>` может быть использована при переходе домена выполнением команд «`sudo`» и «`su`» вместе с «`newrole`», как это предусмотрено для дополнительных доменов пользователей.

Пользовательский домен `<sysadm_t>` является окружением по умолчанию для SELinux-пользователя `<sysadm_u>` и предназначен для использования в качестве дополнительного окружения для SELinux пользователя `<staff_u>`, хотя даже SELinux пользователь `<staff_u>` может настроить подключаемый модуль аутентификации (Pluggable Authentication Module) `< pam_selinux >` для

использования `<sysadm_t>` в качестве его основного домена пользователя.

**Роль `<user_r>` — пользователь системы.**

Пользовательский домен, используемый только в качестве основного. Описание пользователя SELinux `<user_u>` приведено ранее.

Какие-то домены пользователей могут использоваться пользователями для входа в систему, потому что эти домены, например, имеют полномочия по доступу к домашней директории пользователя. Такие домены в предыдущей части назывались основными (`primary`) пользовательскими доменами. Другие домены созданы в качестве дополнительных. Пользователи, используя команды «`sudo`» или «`su`» вместе с «`newrole`», могут осуществить доменный переход (Domain Transition) к этим дополнительным доменам.

Дополнительные домены не могут использоваться для входа в систему. Далее будет продемонстрировано как создаётся такой дополнительный пользовательский домен. Целью является реализовать привилегированную роль SELinux, которой предоставлены полномочия по управлению DNS службой Bind.

Начнём с создания нового дополнительного домена пользователя с названием «`bindadm`», основанного на предустановленном домене SELinux `<webadm_t>`. Новый домен пользователя основан на двух файлах с исходным текстом политики SELinux (SELinux Source Policy):

- `webadm.te`;
- `webadm.if`.

Файлы исходных текстов политики SELinux с расширением `".te"` называются Type Enforcement файлы. Файлы с расширением `".if"` называются интерфейсными (Interface files). Файлы Type Enforcement содержат описания (Declarations) и политику (Policy), персональные или локальные для данного домена (Domain). Интерфейсные файлы содержат описания и политики, общие для этого домена и других доменов, желающими взаимодействовать с данным доменом.

```
mkdir ~/bindadm; cd ~/bindadm
echo "policy_module(bindadm, 0.0.1)" > bindadm.te
echo "role bindadm_r;" >> bindadm.te
echo "userdom_base_user_template(bindadm)" >> bindadm.te
echo "allow bindadm_t self:capability { dac_override
dac_read_search kill sys_ptrace sys_nice " >> bindadm.te
echo "files_dontaudit_search_all_dirs(bindadm_t)" >> bindadm.te
echo "files_manage_generic_locks(bindadm_t) >> bindadm.te
echo "files_list_var(bindadm_t)" >> bindadm.te
echo "selinux_get_enforce_mode(bindadm_t)" >> bindadm.te
echo "seutil_domtrans_setfiles(bindadm_t)" >> bindadm.te
echo "logging_send_syslog_msg(bindadm_t)" >> bindadm.te
echo "userdom_dontaudit_search_user_home_dirs(bindadm_t)" >>
bindadm.te
```

Это основное содержимое для привилегированного дополнительного домена пользователя. Исключена политика, специфичная для управления службой Apache.

Теперь добавим политику, специфичную для управления службой Bind.

Можно позаимствовать эту политику из исходных текстов политики для Bind. Как уже отмечалось, общая политика располагается в интерфейсных файлах. Это значит, что если мы хотим включить общую политику, относящуюся к Bind, можно посмотреть в соответствующем файле политики bind.if. Для включения этой политики в наш Type Enforcement файл требуется всего лишь добавить вызов этого интерфейса:

```
echo "bind_admin(bindadm_t, bindadm_r)" >> bindadm.te
```

На этом Type Enforcement файл bindadm заканчивается. Далее необходимо обеспечить другим доменам возможность взаимодействия с нашим доменом <bindadm\_t>. Реализуем эту часть политики, взяв за основу файл webadm.if.

```
echo "## Bind administrator role" > bindadm.if
echo "#####" >> bindadm.if
echo "## " >> bindadm.if
echo "## Change to the bind administrator role." >> bindadm.if
echo "## " >> bindadm.if
echo '## ' >> bindadm.if
echo "## " >> bindadm.if
echo "## Role allowed access." >> bindadm.if
echo "## " >> bindadm.if
echo "## " >> bindadm.if
echo "## " >> bindadm.if
echo "#" >> bindadm.if
echo "interface(`bindadm_role_change`,`" >> bindadm.if
echo " gen_require(`" >> bindadm.if
echo " role bindadm_r;" >> bindadm.if
echo " `)" >> bindadm.if
echo " allow \"$1 bindadm_r;" >> bindadm.if
echo "')" >> bindadm.if
```

Позже общая политика администратора Bind (Bind Administrator Shared policy) будет использоваться в нашем основном специально созданном пользовательском домене SELinux. Следующим шагом будет создание специализированного пользовательского домена SELinux для обслуживания Bind, разрешающего данному домену осуществлять переход к роли <bindadm\_r> вызовом интерфейса <bindadm\_role\_change>. Создаваемый домен SELinux будет основан на пользовательском домене <staff\_t>, описание политики смотрим в файле staff.te

```
echo "policy_module(bindguy, 0.0.1)" > bindguy.te
echo "role bindguy_r;" >> bindguy.te
echo "userdom_unpriv_user_template(bindguy)" >> bindguy.te
echo "sudo_role_template(bindguy, bindguy_r, bindguy_t)" >>
bindguy.te
```

```
echo "ssh_role_template(bindguy, bindguy_r, bindguy_t)" >>
bindguy.te;
echo "kernel_read_ring_buffer(bindguy_t)" >> bindguy.te
echo "kernel_getattr_core_if(bindguy_t)" >> bindguy.te
echo "kernel_getattr_message_if(bindguy_t)" >> bindguy.te
echo "kernel_read_software_raid_state(bindguy_t)" >> bindguy.te
echo "auth_domtrans_pam_console(bindguy_t)" >> bindguy.te
echo "libs_manage_shared_libs(bindguy_t)" >> bindguy.te
echo "seutil_run_newrole(bindguy_t, bindguy_r)" >> bindguy.te
echo "netutils_run_ping(bindguy_t, bindguy_r)" >> bindguy.te
echo "domain_read_all_domains_state(bindguy_t)" >> bindguy.te
echo "domain_getattr_all_domains(bindguy_t)" >> bindguy.te
echo "domain_obj_id_change_exemption(bindguy_t)" >> bindguy.te
echo "files_read_kernel_modules(bindguy_t)" >> bindguy.te
echo "kernel_read_fs_sysctls(bindguy_t)" >> bindguy.te
echo "modutils_read_module_config(bindguy_t)" >> bindguy.te
echo "modutils_read_module_deps(bindguy_t)" >> bindguy.te
echo "miscfiles_read_hwddata(bindguy_t)" >> bindguy.te
echo "term_use_unallocated_ttys(bindguy_t)" >> bindguy.te
```

Чтобы разрешить домену <bindguy\_t> осуществлять переход в ограниченное окружение SELinux <bindadm\_t>, добавим вызов интерфейса <bindadm\_role\_change>, определённого в нашем интерфейсном файле bindadm.if:

```
echo "bindadm_role_change(bindguy_r)" >> bindguy.te
```

Можно также автоматически создать сопоставление пользователя SELinux с именем <bindguy\_u> ролям <bindguy\_r>, <bindadm\_r> и <system\_r>. Роль <system\_r> включается, чтобы <bindadm\_t> мог остановить, запустить и перезапустить системную службу bind.

```
echo "gen_user(bindguy_u, user, bindguy_r system_r bindadm_r, s0,
s0 - mls_systemhigh, mcs_allcats)" >> bindguy.te
```

Чтобы программы входа знали, что bindguy допустимый пользователь, добавим контексты по умолчанию для этого пользователя, взяв за основу контексты по умолчанию пользователя <staff\_u>:

```
cp /etc/selinux/targeted/contexts/users/staff_u
/etc/selinux/targeted/contexts/users/bindguy_u
sed -i 's/staff/bindguy/g'
/etc/selinux/targeted/contexts/users/bindguy_u
```

Теперь можно собрать и установить обе политики bindguy и bindadm:

```
make -f /usr/share/selinux/devel/Makefile
semodule -i bindguy.pp bindadm.pp
```

Далее командой «useradd», опцией «-Z» и параметром <bindguy\_u> можно создать нового пользователя Linux:

```
useradd -Z bindguy_u bindguy
```

Для того, чтобы разрешить пользователю bindguy использовать команду «sudo» для автоматического перехода к пользователю root и SELinux-домену <bindadm\_t>, добавим в /etc/sudoers:

```
echo "bindguy ALL=(ALL) ROLE=bindadm_r TYPE=bindadm_t ALL" >>
/etc/sudoers
```

При входе пользователя bindguy в систему он оказывается в пользовательском домене <bindguy\_t>, основанном на домене <staff\_t>. Домен <bindguy\_t> может осуществлять переход в домен <bindadm\_t>, используемый с правами root и позволяющий управлять службой Bind.

Например, выполнив следующую команду, пользователь bindguy сможет перезапустить службу bind:

```
service named restart
```

Также пользователю bindguy разрешается редактировать различные конфигурационные файлы и файлы информационного наполнения Bind. При этом, например, пользователь bindguy не имеет прав изменить пароль пользователя root.

Подведём итог. Процессы и файлы маркируются метками – контекстом SELinux, который содержит информацию: пользователь SELinux, роль, тип и уровень (опционально). Когда SELinux включён, вся эта информация используется для принятия решения о предоставлении доступа.

В контексте SELinux используется следующий синтаксис SELinux

```
<user>:<role>:<type>:<level>:<пользователь_SELinux >
```

<Пользователь\_SELinux> – это сущность, определённая в политике, которая отвечает за определённый набор ролей и за определённый набор MLS-уровней. Каждый пользователь ОС сопоставлен пользователю SELinux посредством политики SELinux. Это позволяет пользователям наследовать ограничения, установленные на пользователей SELinux. Сопоставленные сущности пользователей SELinux используются в контексте SELinux для процессов в сессии, в порядке определения для каких ролей и уровней они применимы.

Роль – это часть модели безопасности Ролевого управления доступом Role-Based Access Control (RBAC). Роль – это атрибут RBAC. Пользователи SELinux авторитетны для ролей, а роль авторитетна для доменов. Определённая роль определяет, какие домены могут быть доступны для пользователей с этой ролью. Роль служит промежуточным звеном между доменами и пользователями SELinux. Роль, которой обладает пользователь, определяет, в какие домены может попасть пользователь – фактически, этот механизм управляет доступностью объектов. Таким образом, уменьшается риск, связанный с уязвимостью

повышения привилегий в системе. По умолчанию пользователям назначена неопределённая роль, не накладывающая ограничений на пользователя. Но есть и предопределённые роли пользователя и администратора системы, которые могут быть назначены администратором для повышения безопасности системы.

Тип – это атрибут `Type Enforcement`. Тип определяет домен для процессов и тип для файлов. Правила политики SELinux определяют, как типы взаимодействуют друг с другом, является ли тип доменом, получающим доступ к типу, или доменом, получающим доступ к другому домену. Доступ разрешается, только если существует определённое правило политики SELinux, позволяющее данное действие.

Контекст безопасности записывается в атрибуты файла (в файловой системе) и создаётся при установке SELinux (операция `labeling`). Уже присвоенный контекст безопасности может быть впоследствии изменён - операцией «`transition`».

# Сеть и служебные программы

## 8. Настройка сети

Настройка сети в РЕД ОС производится с помощью программы Network Manager. Для ручной настройки сетевого адаптера необходимо в графическом интерфейсе рабочего стола РЕД ОС на системной панели в разделе апплетов нажать правой кнопкой мыши по значку апплета «Network Manager» (рисунок 8.1).

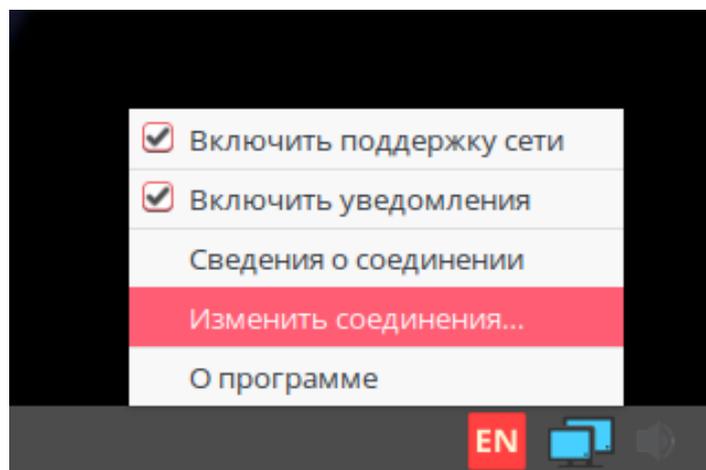


Рисунок 8.1 – Запуск утилиты настройки сетевых соединений

В открывшемся окне утилиты «Сетевые соединения» необходимо выделить нужный сетевой адаптер и нажать на кнопку с изображением шестеренки «Изменить выбранное соединение» внизу окна (рисунок 8.2).

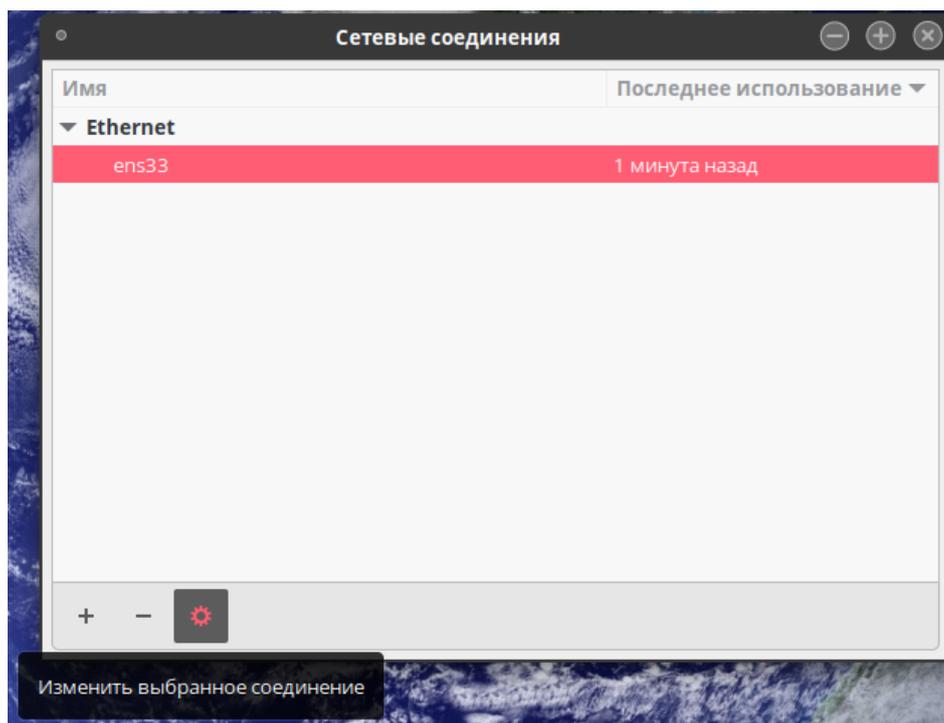


Рисунок 8.2 – Изменение сетевого адаптера

В открывшемся окне свойств сетевого адаптера (рисунок 8.3) можно установить свойства автоматического подключения - «Подключаться автоматически» и «Доступно всем пользователям», во вкладке «Параметры IPv4» задать ручную задания метрики сетевого подключения, нажав кнопку «Добавить».

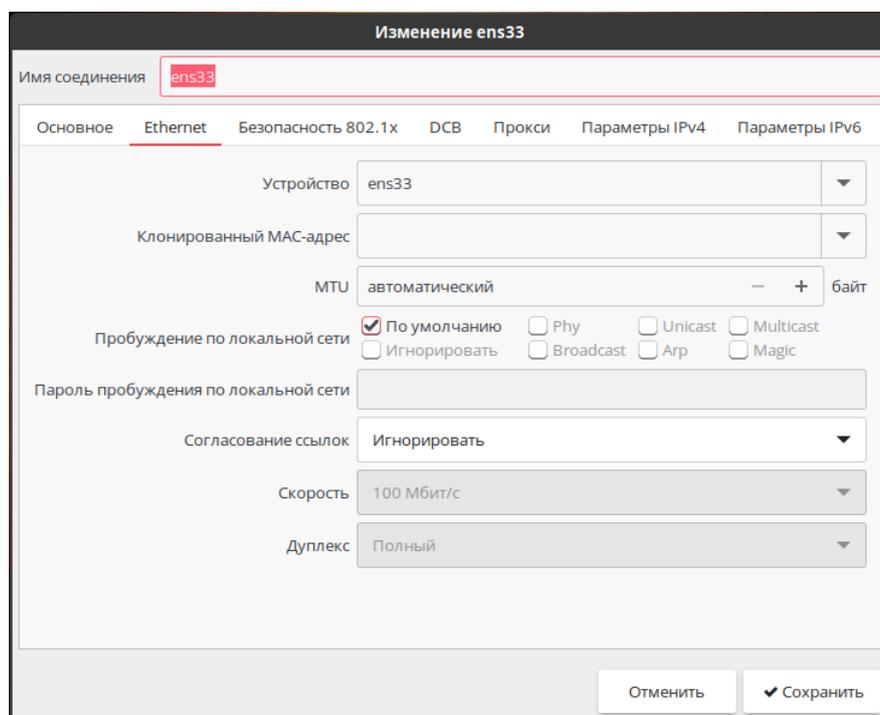


Рисунок 8.3 – Изменение свойств сетевого адаптера

Для подтверждения изменений необходимо нажать кнопку «Сохранить».

Для того чтобы изменения вступили в силу, необходимо переподключить сетевое соединение или перезапустить службу NetworkManager.

Для настройки сети в консоли нужно установить пакет net-tools.

Для просмотра сетевых настроек нужно ввести команду:

```
ifconfig
```

Или воспользоваться командой ip с параметром addr:

```
ip addr
```

Тут можно увидеть параметры и название сетевой карты.

Допустим, необходимо сменить или установить ip-адрес. Для этого переходим в директорию /etc/sysconfig/network-scripts и открываем на редактирование файл устройства. Этот файл имеет примерно следующее содержание:

```
cat ifcfg-eno16777736
TYPE=Ethernet
BOOTPROTO=dhcp
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=no
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPV6_FAILURE_FATAL=no
NAME=eno16777736
UUID=dc1636be-5281-4a07-8681-fcdc8b161c8c
DEVICE=eno16777736
ONBOOT=no
PEERDNS=yes
PEERROUTES=yes
```

Для установки статического IP-адреса нам необходимо на строчке BOOTPROTO установить

```
BOOTPROTO=none
```

и дописать:

- Указать ДНС:

```
DNS1=8.8.8.8
```

- Указать IP:

```
IPADDR0=172.16.0.30
```

- Указать нужную маску:

```
PREFIX0=24
```

- И шлюз по умолчанию:

```
GATEWAY0=172.16.0.1
```

- И чтобы сетевая карта активировалась при запуске ОС, необходимо в этом файле найти параметр ONBOOT и установить ему «yes».

Для немедленного применения изменений перезапустим сеть:

```
/etc/init.d/network restart
```

Предположим, что сетевая карта настроена на статический IP, а вы хотите получать настройки по DHCP. Переходим в папку `/etc/sysconfig/network-scripts` и открываем файл на редактирование с названием вашей сетевой карты. Находим там и удаляем параметры «DNS», «IPADDR», «PREFIX», «GATEWAY», а в параметре `BOOTPROTO` указываем значение «dhcp».

В файл настройки сетевой карты можно добавить столько DNS серверов, сколько требуется. Например:

```
DNS1=172.16.0.1
DNS2=8.8.8.8
DNS3=8.8.4.4
```

Проверить шлюз, по умолчанию установленный в системе:

```
netstat -nr
```

```
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
0.0.0.0 172.16.0.1 0.0.0.0 UG 0 0 0 eno16777736
172.16.0.0 0.0.0.0 255.255.255.0 U 0 0 0 eno16777736
```

Строка с «Destination 0.0.0.0» определяет адрес шлюза. Если у вас ее нет, либо в поле «Gateway» установлен неверный шлюз, то можно это изменить. Устанавливаем шлюз по умолчанию:

```
route add default gw 172.16.0.1
```

Если вы не сменили при установке имя сервера или вы хотите его изменить, то сделать это можно следующим образом. Для начала проверим, какой `hostname` у нас установлен:

```
hostname
```

Допустим, мы хотим изменить имя: `server.work`, для этого необходимо отредактировать файл `/etc/hostname` или использовать команду:

```
hostnamectl set-hostname name
```

Для смены hostname перезагрузка не требуется.

После того, как TCP-пакеты были переданы ОС, среди других действий, их обрабатывают два файла - /etc/hosts.allow и /etc/hosts.deny. Эти два файла работают так же, как и стандартные правила брандмауэра. Первоначально демон tcpd обрабатывает пакеты пропуская их через содержимое файла hosts.allow, а затем через файл hosts.deny.

Синтаксис этих файлов:

```
<служба>: <IP-адрес> или <имя_хоста>
```

Так, например, если необходимо заблокировать все smtp-пакеты, идущие от test.ru, необходимо ввести в файл hosts.deny следующую строчку:

```
smtp: test.ru
```

Мы можем также указать вместо имени хоста его IP-адрес (лучше всего физический):

```
smtp: 192.168.1.10
```

Можно использовать знак «.» в строке адреса, для обозначения сети. К примеру, если мы хотим разрешить доступ по http из всей сети 192.168.10.0/24, то мы должны написать в hosts.allow следующее:

```
http: 192.168.10
```

Также мы можем использовать этот знак, если хотим разрешить доступ к какой-либо службе всем компьютерам нашего домена, указав в hosts.allow следующее:

```
http: .test.ru
```

## 9. Служебные программы

### 9.1 Служба xinetd

Служба xinetd запускает процессы, которые предоставляют различные сервисы сети Интернет. В отличие от сервисов, которые стартуют во время инициализации системы и пребывают в бездействии в ожидании запросов, xinetd представляет собой только один процесс, слушающий на всех портах сервисов, перечисленных в файле конфигурации xinetd.conf. Когда приходит запрос, xinetd запускает соответствующий сервер. По причине такой работы xinetd называют ещё супер-сервером.

Сервисы, перечисленные в конфигурационном файле xinetd можно разделить на две группы.

Сервисы из первой группы называются multi-threaded, и на каждый новый запрос запускается новый серверный процесс. Для таких сервисов xinetd продолжает слушать сеть на соответствующем порту, ожидая новых запросов и готовый породить новый процесс.

В другую группу включаются сервисы, службы которых в состоянии обрабатывать новые соединения. Такие сервисы называются single-threaded, и xinetd прекращает обработку новых запросов до тех пор, пока серверный процесс не завершит свою работу. Сервисы в этой группе обычно datagram-based.

Итак, причиной существования супер-сервера является факт сохранения системных ресурсов за счёт не запуска множества серверных процессов, которые, возможно, будут бездействовать большую часть своей жизни. Полностью соответствуя назначению запускать требуемые сервисы, xinetd осуществляет так же функции контроля доступа и регистрации событий. Кроме того, xinetd не ограничен сервисами, перечисленными в файле /etc/services. Можно использовать xinetd для запуска сервисов специального назначения.

## 9.1.1 Параметры

Параметр	Значение параметра
-d	Активирует режим отладки. Этот параметр выводит много отладочной информации и позволяет отладить работу xinetd.
-syslog <syslog _facility>	Этот параметр разрешает регистрацию событий, используя syslog. Сообщения, производимые службой xinetd, регистрируются, используя одну из syslog_facility. Поддерживаются следующие facility: daemon, auth, user, local [0-7]. Эта опция не действует, если активирован режим отладки, так как при отладке все сообщения посылаются на консоль.
-filelog <logfile>	Производимые xinetd сообщения помещаются в указанный файл. Новые сообщения всегда добавляются к существующим. Если файл не существует, то он создаётся. Опция не действует в режиме отладки.
-f <config_file>	Определяет положение файла конфигурации xinetd. По умолчанию - это /etc/xinetd.conf.
-pid	Идентификатор процесса (PID) выводится на устройство стандартной ошибки. Не действует в режиме отладки.
-loop <rate>	Этот параметр устанавливает ограничение скорости запуска серверов, указывается число запускаемых серверов в секунду. При превышении указанного значения запуск новых процессов блокируется, и сервис становится временно недоступным. Значение этого параметра определяется производительностью компьютера. По умолчанию - 10.
-reuse	Если указан этот параметр, то xinetd устанавливает <SO_REUSEADDR> для сокета, используемого сервисом. Это позволяет использовать адрес, даже если активны программы, которые уже его используют. Это может случиться, когда предыдущая копия xinetd пытается запустить сервер, который уже выполняется. Параметр не эффективен с RPC-сервисами.
-limit <proc_limit>	Этот параметр устанавливает предел на число одновременно выполняющихся процессов, запущенных службой xinetd. Использование параметра позволяет предотвратить переполнение таблицы процессов.
-logprocs <limit>	Параметр устанавливает максимальное значение одновременно выполняемых процессов, запущенных по запросу удалённого userid.
-shutdownprocs <limit>	Параметр устанавливает предельное число одновременно выполняющихся серверов сервиса shutdown (concurrently running servers for service shutdown).

Параметр	Значение параметра
-cc <interval>	Параметр задаёт промежуток времени в секундах, через который xinetd производит периодическую проверку внутренней целостности.

Параметры <syslog> и <filelog> взаимно исключают друг друга. Если ничего не указано, то по умолчанию используется syslog daemon facility. Не путайте сообщения xinetd с сообщениями, относящимися к функциям регистрации событий. Последние журналируются, только если это указано в файле конфигурации.

### 9.1.2 Управление xinetd

Служба xinetd выполняет определённые действия при получении определённых сигналов. Действия, ассоциированные с соответствующими сигналами, могут быть переопределены путём редактирования config.h и последующей компиляции.

**SIGUSR1**

Вызывает «мягкую» переконфигурацию. Это означает, что xinetd перечитывает файл конфигурации и подстраивается под изменения.

**SIGUSR2**

Вызывает «жёсткую» переконфигурацию. Это значит то же самое, что и «мягкая» переконфигурация, за исключением того, что все серверы для сервисов, которые стали недоступны, принудительно завершаются. Контроль доступа заново выполняется для выполняющихся серверных процессов путём проверки удалённого хоста, времени доступа и количества выполняющихся серверов. Если число выполняющихся процессов превышает заданное, произвольным образом выбранные процессы «убиваются», чтобы число оставшихся удовлетворяло поставленному условию. Также, если флаг «INTERCEPT» был сброшен или установлен, все серверы, обеспечивающие этот сервис, завершаются. Все это выполняется для того, чтобы после «жёсткой» реконфигурации не осталось ни одного работающего процесса, обрабатывающего запросы с адресов, не соответствующих критериям контроля доступа.

Сигнал	Описание сигнала
SIGQUIT	приводит к завершению программы.
SIGTERM	завершает все выполняющиеся серверы перед завершением xinetd.
SIGHUP	приводит к генерации дампа внутреннего состояния (по умолчанию файл дампа /tmp/xinetd.dump).
SIGIOT	вызывает проверку внутренней целостности, чтобы проверить, что структуры данных, используемые программой, не повреждены. После завершения проверки xinetd генерирует сообщение о результате проверки.

При реконфигурации лог-файлы закрываются и вновь открываются. Это позволяет удалять старые логи.

### 9.1.3 Файлы

`/etc/xinetd.conf` – стандартный конфигурационный файл.

`/var/run/xinetd.dump` – стандартный файл дампа.

## 9.2 Crontab

Crontab - таблицы, управляющие работой службы «cron». Файл содержит инструкции службы «cron» в общей форме: запускать указанную команду в заданное время и в заданные дни. На компьютере обычно имеются общесистемный файл (`/etc/crontab`), и индивидуальные файлы (`/var/cron/tabs/<имя-пользователя>`) для пользователей системы. Таким образом, команды в файле будут выполняться с правами этих пользователей или, в случае общесистемного файла, с правами пользователя, указанного в командной строке при запуске службы. У служб «Uucp» и «News» обычно есть свои собственные «crontab», устраняющие необходимость в явном запуске «su» в рамках команды «cron».

Хотя «cron», по сути, является обыкновенным текстовым файлом, он не должен редактироваться обычными средствами. Для создания, изменения и удаления следует использовать специальную утилиту, «crontab».

Пустые строки, ведущие пробелы и символы табуляции игнорируются. Строки, начинающиеся с символа «#», считаются комментариями и игнорируются. Заметьте, что комментарии не допускаются в тех же строках, где расположены команды «cron», так как они будут распознаны как части команды. По этой же причине комментарии не разрешены в строках, задающих переменные среды.

Строка-директива представляет собой либо задание переменной среды, либо команду «cron».

Можно определять среду (набор переменных среды), в которой будет выполняться команда. Задание переменной среды осуществляется в следующей форме:

```
<имя_переменной> = <значение>
```

где пробелы вокруг знака равенства («=») не обязательны, и любые пробелы после значения будут использованы как часть значения переменной `<имя_переменной>`. Строка `<значение>` может быть заключена в кавычки (одинарные или двойные) для возможности сохранения пробелов в начале и конце.

Несколько переменных среды устанавливаются автоматически службой «cron». SHELL устанавливается в `/bin/sh`, а LOGNAME и HOME определяются по файлу `/etc/passwd` (в соответствии с владельцем crontab). Значения переменных HOME и SHELL можно переопределить директивами «crontab».

В дополнение к LOGNAME, HOME и SHELL «cron» может использовать переменную `<MAILTO>` в случаях, если в данном «crontab» была указана отправка почты. Если `<MAILTO>` определена (и не пуста), электронная почта отправляется указанному в переменной пользователю. Если `<MAILTO>` определена, но пустая, (`MAILTO = ' '`), электронная почта отправляться не будет.

В противном случае, почта посылается владельцу «crontab». Эта переменная полезна при запуске команд от псевдопользователей, для которых не определены почтовые адреса в системе.

Формат команд «cron» аналогичен стандарту V7 и является совместимым с ним. Существует две конфигурации «cron»: системная и пользовательская. Общесистемная настройка «crontab» работает безусловно для всех пользователей РЕД ОС. Пользовательская настройка является дополнительной и выполняется в сессиях пользователей.

Каждая строка в системной конфигурации «cron», расположенной в каталоге /etc, состоит из шести полей и команды:

```
<минута> <час> <число> <месяц> <день_недели> <пользователь>
<команда>
```

Каждая строка в пользовательской конфигурации «cron», расположенной в домашнем каталоге пользователя состоит из пяти полей и команды:

```
<минута> <час> <число> <месяц> <день_недели> <команда>
```

Поля отделяются друг от друга пробелами или символами табуляции. Команда может состоять из нескольких полей. Допустимые значения полей:

Поле	Допустимые значения
<минута>	* или 0-59
<час>	* или 0-23
<число>	* или 1-31
<месяц>	*, 1-12 или имя месяца (см. ниже)
<день_недели>	*, 0-7 или имя дня (воскресенье - это 0 и 7)
<пользователь>	имя существующего пользователя
<команда>	строка

Допустимо указание нескольких значений (и диапазонов через тире) через запятую. Примеры:

```
' '1, 2, 5, 9' ' '0-4, 8-12'
```

Диапазон указывается как два числа, разделённых дефисом. Указываемые числа включаются в диапазон. Например, значение поля <час> 8-11 приведёт к выполнению команды в 8, 9, 10 и 11 часов.

При указании диапазона можно пропускать некоторые его значения, указав шаг в форме /<число>.

Например:

```
' '0-23/2'
```

для поля <час> означает запуск команды через два часа (по стандарту V7

пришлось бы указывать "0,2,4,6,8,10,12,14,16,18,20,22").

Шаг можно указывать также после звёздочки - "каждые два часа" соответствует значению:

```
''*/2''
```

Звёздочка («\*») без шага соответствует полному диапазону значений.

Для задания полей <месяц> и <день\_недели> можно использовать имена. Указывайте первые три буквы нужного дня или месяца на английском, регистр букв не имеет значения. Диапазоны или списки имён не разрешены.

Поле <команда> (остаток строки) определяет запускаемую по расписанию команду - вся оставшаяся часть строки до символа перевода строки или символа «%». Будет выполнен вызов /bin/sh или другой оболочки, определённой в переменной SHELL в «crontab». Знак процента («%») в команде (если он не экранирован обратной косой чертой («\»)), будет соответствовать символу перевода строки и все данные после первого «%» будут посланы для команды на стандартный ввод.

Служба «cron» запускает команды, когда значения полей <минута>, <час>, <месяц> и хотя бы одно из полей <число> и <день\_недели>, совпадают с текущим временем (см. замечание ниже). Служба «cron» сверяет директивы с текущим временем раз в минуту.

**Примечание.** День выполнения команды может быть задан в двух полях - <число> и <день\_недели>. Если оба поля определены (т.е. не равны \*), то команда будет запущена, когда любое поле совпадёт с текущим временем.

Например, запись:

```
30 4 1,15 * 5
```

приведёт к выполнению команды в 4:30 по полуночи первого и пятнадцатого числа каждого месяца, плюс в каждую пятницу.

Вместо первых пяти полей допустимо указание одного из восьми специальных триггеров:

Строка	Значение
@reboot	Выполнить команду один раз, при запуске cron(8).
@yearly	Выполнять команду каждое 1 января, «0 0 1 1 *».
@annually	(эквивалентно @yearly).
@monthly	Выполнять команду в начале каждого месяца, «0 0 1 * *».
@weekly	Выполнять команду каждое воскресенье, «0 0 * * 0».
@daily	Выполнять команду в полночь, «0 0 * * *».
@midnight	(эквивалентно @daily).
@hourly	Выполнять команду раз в час, «0 * * * *».

## 9.3 Полноэкранный редактор vi

Редактор vi - универсальный полноэкранный текстовый редактор.

Имеющиеся на многих типах терминалов функциональные клавиши практически не используются. Если клавиатура терминала имеет стрелочные клавиши, то они используются, но в ограниченном контексте.

### 9.3.1 Режимы работы редактора

#### Ввод текста

В этом режиме все, что набирается на клавиатуре, отображается на экране терминала и запоминается в буфере редактора.

В данном режиме нет возможности осуществлять операции редактирования текста, за исключением стирания последнего набранного символа (с помощью комбинации клавиш «Ctrl+N»).

#### Командный режим

В этом режиме символы клавиатуры выполняют специальные функции (перемещение курсора, стирание частей текста, и т. д.), то есть функции редактирования.

В данном режиме набираемые команды не отображаются на экране.

#### Режим командной строки

Режим командной строки позволяет производить более глобальные операции с текстом: записывать отредактированный текст в файл, считывать новый файл, выходить из vi, производить настройку редактора, поиск по шаблону, а также осуществлять некоторые функции редактирования.

Команды отображаются в нижней части экрана (в командной строке редактора).

### 9.3.2 Ввод текста

Действие	Описание действия
«Return»	создаёт пустую строку и переводит курсор в ее начало;
«Ctrl+N»	уничтожает последний введённый символ (это действие не отображается на экране до выхода в командный режим);
«Ctrl+[» или «Esc»	переводят редактор в командный режим.

В режиме ввода текста стрелочная клавиатура не работает.

### 9.3.3 Команды

Команда	Описание команды
i	переход в режим набора методом вставки перед текущим символом;
a	переход в режим набора методом вставки за текущим символом;
R	переход в режим набора текста методом набивки.

### 9.3.4 Перемещение курсора

Действие	Описание действия
h, j, k, l	на один символ (одну строку), как показано стрелками;
^ или 0	в начало текущей строки;
\$	в конец текущей строки;
w	на слово вправо;
b	на слово влево;
}	на параграф вперёд (параграф – это блок текста, отделённый пустой строкой);
{	на параграф назад;
[[	в начало текста;
]]	в конец текста.

Кнопки стрелочной клавиатуры также позволяют перемещаться по тексту.

### 9.3.5 Редактирование

Действие	Описание действия
dd	стирание текущей строки;
d <движение_курсора>	стирание от текущего положения курсора до нового, задаваемого символом перемещения курсора. Нажатие кнопок стрелочной клавиатуры не является движением курсора и не может использоваться в комбинированных командах;
J	слияние текущей строки со следующей;
u	отмена последней команды;
.	повтор последней команды;
:	переход в режим командной строки.

### 9.3.6 Командная строка

Опция	Значение опции
<code>:q</code> или <code>:q!</code>	выход из редактора без сохранения изменений;
<code>:x</code>	выход из редактора с записью, если файл был модифицирован;
<code>:w</code> или <code>w &lt;filename&gt;</code> или <code>w! &lt;filename&gt;</code>	запись файла и возвращение в командный режим;
<code>:e &lt;filename&gt;</code> или <code>:e!</code> <code>&lt;filename&gt;</code>	загрузка файла <code>&lt;filename&gt;</code> ;
<code>:r &lt;filename&gt;</code>	добавить содержимое указанного файла к редактируемому сразу за текущей строкой;
<code>:set nu</code>	включить нумерацию строк;
<code>:set nonu</code>	отключить нумерацию строк;
<code>!:command</code>	выполнить команду UNIX не покидая редактора;
<code>:/&lt;word&gt;</code>	выполнить поиск слова <code>&lt;word&gt;</code> в тексте;
<code>:/</code>	повторить поиск слова <code>&lt;word&gt;</code> далее по тексту.

### 9.3.7 Блоки, буферы, окна редактирования. Повторители

#### Повторители

Командам и движениям курсора можно давать повторители (числа), например:

Команда	Описание команды
<code>2w</code>	передвинуть курсор на два слова вперёд;
<code>10l</code>	передвинуть курсор на десять символов вправо;
<code>d10l</code>	стереть десять символов справа от курсора;
<code>2d10l</code>	стереть двадцать символов справа от курсора;
<code>5J</code>	слить пять последующих строк в одну;
<code>4.</code>	повторить последнюю введённую команду четыре раза;

#### Буферы vi

Редактор имеет три типа буферов: буфер стирания (0-9), неименованный буфер и именованные буферы (a-z).

В буферы стирания автоматически заносятся стираемые элементы. В буфере «0» хранится последний стёртый элемент, в буфере «1» - предпоследний и т. д. Занести в буфер:

Опция	Значение опции
уу	занести текущую строку в неименованный буфер;
у <движение_курсора>	занести указанный движением курсора блок текста в неименованный буфер;
"ауу	занести текущую строку в именованный буфер а;
"Ауу	добавить текущую строку к содержимому именованного буфера а;
"бу10j	занести последующие 10 строк в именованный буфер b.

Вставить из буфера:

Команда	Описание команды
р	вставить в текущую позицию содержимое неименованного буфера;
"ар	вставить в текущую позицию содержимое именованного буфера а;
"1р	вставить в текущую позицию содержимое буфера стирания 1.

### Многооконное редактирование

Редактировать сразу несколько файлов можно либо пользуясь командной редактора :e <filename>, либо указав все необходимые файлы в командной строке при вызове редактора (например: vi <file1> <file2> <file3>). В последнем случае вы двигаетесь по списку файлов с помощью команд:

Команда	Описание команды
:n	переход к следующему файлу в списке;
:rew	возврат к редактированию первого файла в списке.

Именованные буферы сохраняют своё содержимое при переходе к редактированию другого файла.

### 9.3.8 Открыть/создать файл

- vi мама.ра.а.txt – открыть один файл.
- vi мама.txt ра.а.txt – открыть файл мама.txt, после выхода из него открыть файл ра.а.txt.

Файл открывается в командном режиме с помощью команды vi. Здесь мы можем просмотреть файл, переместиться по его содержимому, стереть текст, но внести изменения или ввести текст в этом режиме нельзя.

Создание файла происходит при помощи той же команды. Создание файла происходит в момент сохранения.

Для открытия или создания нового файла в командном режиме необходимо выполнить команду:

```
:e <имя_файла>
```

Перед этим нужно сохранить предыдущий файл:

Команда	Описание команды
:w	сохраняет файл с существующим именем;
:sav <имя_файла>	«Сохранить как».

### 9.3.9 Дополнительные опции

Дополнительные возможности редактора:

Команда	Описание команды
G	перейти в конец файла
<number>G	перейти на конкретную строку <number>
:<number>	перейти на <number> строк вперед
:set nu[mber]	отобразить слева нумерацию строк (^ nonu[mber] - спрятать нумерацию)
:set wrap	переносить длинные строки (:set nowrap - не переносить)
:syntax on/off	включить/выключить подсветку синтаксиса
:colorscheme <name>	задать цветовую тему (где <name> - имя темы, «ТАВ» работает как авто-дополнение)
/мама	поиск текста «мама» в файле
n	повторить поиск
:h или :help	список возможной помощи (:viusage, :exusage)
:set fileformat=dos	привести концы строк в файле к виду dos или unix, соответственно
:set fileformat=unix	
:set ts=4	задать размер табуляции в 4 пробела

## 9.4 Редактор ViM

### 9.4.1 Режимы работы

В ViM существуют 3 режима работы:

**Основной** – предназначен для просмотра файла, ввода команд и перехода из него в другие режимы. Из любого режима в командный можно попасть при нажатии «ESC». При нажатии клавиши «:» становится доступна командная строка ViM, в которой можно вводить команды. Основные команды – команда выхода «quit» (ViM понимает сокращения, поэтому можно давать команду одной

буквой «q»), команда сохранения «write» (или «w»), параметром которой может быть имя файла, и вызов справки по, очевидно, «help» (или «h»). На остальные клавиши (и их последовательности) можно присвоить любое действие, либо использовать значения по умолчанию.

**Визуальный** – предназначен, в первую очередь, для выделения блоков текста. Для запоминания предлагаются 3 варианта перехода в этот режим – клавишей «v» для посимвольного выбора, «Shift+V» для построчного и «Ctrl+V» для блочного. В нормальном режиме (при переходе по «v») можно оперировать следующими сущностями: слово («w»), предложение («s»), параграф («p») и блок («b»). Выделение при этом начинать с позиции курсора («a»), или же с начала блока («i»). Например, выделение текущего блока (участка, ограниченного парными элементами) можно произвести следующим образом «Esc+VIB». Копирование в буфер выделенного текста осуществляется по «u», вырезание по «d», а вставка соответственно «p».

**Режим редактирования** – переход в режим редактирования осуществляется нажатием клавиши «Ins».

### 9.4.2 Основные возможности

Все возможности и команды редактора ViM перечислить весьма затруднительно. Перечисленные ниже команды вводятся в основном режиме (если нет специального уточнения). Все они имеют команднорочные аналоги и могут быть легко переопределены пользователями.

#### Переходы

Для перехода на строку с номером n воспользуйтесь командой «G». Так, для перехода к началу текста наберите 0G, для сотой строки 100G, а для конца документа - \$G. Для перехода на n символов в нужную вам сторону можете использовать клавиши со стрелками. То есть для перехода на 1000 символов вниз наберите «1000» и нажмите стрелку «вниз».

Для перемещения по тексту используйте следующие команды:

Команда	Описание команды
(, )	для перемещения по предложениям;
{, }	для параграфов;
[[, ]]	для функций;
%	переход к парной скобке;
", "	к предыдущему положению;
CTRL+O, CTRL+I	соответственно назад и вперёд по истории переходов.

#### Метки

Используются для отметки позиции ^<метка>, где <меткой> является любая буква, и быстрого к ней перехода (метка). Метки нижнего регистра действительны в пределах данного файла, метки же верхнего регистра действуют

во всех открытых файлах. Список всех меток можно получить командой «marks».

### Регистры

В редакторе доступно множество именованных регистров (хранилищ данных, буферов). Регистр отмечается «"<буква>». К нему применимы все стандартные действия - копирование в него ("<метка> y), вырезание ("<метка> ^) и вставка из него ("<метка> p, можете вместо p использовать [p,]p для вставки соответственно перед или после курсора). В режиме редактирования вставка из регистра осуществляется по ««Ctrl+R» <метка>». Для добавления данных в регистр используйте заглавную метку.

Также вы можете писать в регистр, воспользовавшись командой «^метка» и завершая запись по «q». Таким образом, вы сохраняете макрос, выполнить который можно по «@метка».

Регистры с метками «\*» и «+» совпадают с X-Window clipboards, «%» - соответствует редактируемому файлу. Для просмотра содержимого всех регистров воспользуйтесь командой:

```
:registers
```

либо

```
:reg <метка1><метка2>...
```

для просмотра некоторых.

### Фолды

Предназначены для сокрытия ненужных в данный момент данных, дабы те не отвлекали внимание. Например, кода подпрограммы, с которой вы в данный момент не работаете. По умолчанию фолды активированы в режиме их ручной расстановки. Если вы хотите их автоактивации по отношению к табуляции, то добавьте в конфиг строку:

```
set foldmethod=indent
```

Все команды для работы с фолдами начинаются с «z». Открытие фолда производится, например, по «zo» (или стрелке вправо) на нем, закрытие кода в фолд - по «zc».

### Сессии

При ведении группы проектов нередко желательно сохранить текущее состояние и настройки редактора, чтобы в дальнейшем продолжить работу с того же места. Для этого и предназначены сессии, что создаются командой:

```
:mksession /path/to/Session.vim
```

а читаются простой командой:

```
:so /path/to/Session.vim
```

Гораздо чаще, впрочем, возникает нужда в сохранении не всей сессии, но только текущего контекста (во что входит, например, положение курсора в коде, текущая расстановка фолдов и много другое, о чем читайте в документации). Это действие выполняет команда:

```
:mkview
```

чтение:

```
:loadview
```

Очень удобно сделать сохранение и чтение контекста автоматическим при начале и окончании редактирования файла. Это может быть реализовано следующим кодом (применяется для всех файлов, имеющих точку в имени):

```
au BufWinLeave *.* mkview au BufWinEnter *.* silent loadview
```

### Поиск и замена

Поиск осуществляется командами «/» для поиска (по регулярному выражению) вперёд, а «?» в обратном направлении. Для продолжения поиска используйте «n», а для прошлого варианта «N». Для поиска слова под курсором используются соответственно «#» и «\*».

Для поиска с заменой используйте `^s^TО/м что/gic`, где «%» означает работу со всем текстом (а не с текущей строкой), «g» – глобальная замена (а не первое совпадение), «i» – игнорирование регистра, а «c» – подтверждение каждого действия.

### Автодополнение

Производится по содержимому данного файла, а также указанных в переменной `<dictionary>` по нажатию клавиш `"`.

### Отмена

«u» – для отмены и `"` – смены регистра.

«~» – для выделенного участка (или буквы под курсором).

«U» – принудительно установить верхний регистр, а «u», соответственно, нижний.

### Повторить

«.».

### 9.4.3 Конфигурация

Основным конфигурационным файлом является `~/vimrc`. Активация русского шрифта в GUI-режиме, плюс выбор темы для обоих режимов осуществляется, например, следующим кодом:

```
if has(<gui_running>)
  colorscheme candy
  set guifont=-cronyx-courier-medium-r-normal-*-*-120-*-*-m-*-koi8-
r endif
```

```
if !has(<gui_running>) colorscheme elflord endif
```

Перечень наиболее используемых «горячих» клавиш:

- Выход по F10:

```
nmap <F10> :q<CR>
imap <F10> <ESC>:q<CR>
```

- Сохранение по F2:

```
nmap <F2> :w>CR?
imap <F2> <ESC>:w<CR>i<Right>
```

- Компиляция по F9:

```
nmap <F9> :make<CR>
imap <F9> <ESC>:make<CR>
```