Инструкция по установке и эксплуатации
ПО АСТД 37С
(в составе ОС «Циркон 37С» и ПО «Циркон 37Т»)

СОДЕРЖАНИЕ

1. Аппаратные требования

1.1. Технические требования к конфигурации компьютера

Требования для обеспечения работы ПО АСТД 37С предъявляются к вычислительным ресурсам используемых технических средств, минимальные и рекомендуемые параметры которых приведены в таблице 1.

Таблица 1 – Технические требования к конфигурации компьютера

Наименование устройства (характеристики)	Минимальные значения параметров	Рекомендуемые значения параметров
Требования к конфигурации компьютера		
Процессор	Разрядность x86-64, производитель AMD или Intel, тактовая частота 2 ГГц, 2 ядра	Разрядность x86-64, производитель AMD или Intel, тактовая частота 3 ГГц, 4 ядра
Оперативная память	2 Гбайт	4 Гбайт
Объем свободного дискового пространства на HDD	8 Гбайт	16 Гбайт
Устройство чтения DVD-дисков	DVD-ROM / USB drive	DVD-ROM / USB drive
Сетевой контроллер	Ethernet-адаптер с пропускной способностью от 1 Гбит/с	Ethernet-адаптер с пропускной способностью от 1 Гбит/с
Видеокарта	С поддержкой OpenGL и объемом памяти от 128 Мбайт	С поддержкой OpenGL и объемом памяти от 128 Мбайт
Требования к рабочим местам для работы ОС «Циркон 37С»		
Устройства взаимодействия с пользователем	Клавиатура и мышь	Клавиатура и мышь
Монитор	Стандартный монитор SVGA 15"	Стандартный монитор SVGA 19"
Разрешение экрана	1280 × 1024 px	1920 × 1080 px

Для функционирования ПО «Циркон 37Т» на терминальном устройстве необходима конфигурация терминального устройства не хуже приведенной в таблице 2.

Таблица 2 – Требования к терминальному устройству

Устройство	Ограничения
Процессор	NXP i.mx6 4x1Ггц
ОЗУ	2 Гбайт
PCI устройства	Сетевой адаптер
Карт-ридер	Поддерживается использование смарт-карт типа ACOS и ESMART

Ограничения (в виде виртуальных аппаратных средств) накладываемые на виртуальные машины представлено в таблице 3.

Таблица 3 – Ограничения, накладываемые на виртуальные ресурсы гипервизора

Виртуальное устройство	Ограничения
Процессор	Максимально поддерживается 160 виртуальных процессоров
ОЗУ	Объем ОЗУ зависит от требований, предъявляемых к операционной системе и приложениям, функционирующим под ее управлением. На одну виртуальную машину может быть выделено от 512 Мбайт до 512 Гбайт ОЗУ
НЖМД	Для каждой виртуальной машины поддерживается до 28 виртуальных НЖМД (3 IDE и 25 virtio)
PCI устройства	Поддерживается до 31 PCI устройства на одну виртуальную машину

1.2. Дополнительные требования к аппаратному оборудованию

Дополнительные технические требования, предъявляемые к аппаратному обеспечению для работы ОС «Циркон 37С», имеют следующие параметры:

- Концентратор локальной вычислительной сети (ЛВС). Для обеспечения функционирования ОС «Циркон 37С» в рамках локальной вычислительной сети Ethernet необходимо наличие концентратора ЛВС (Hub или Switch), удовлетворяющего следующим условиям: количество портов RJ-45 не менее одного на каждый подключаемый компьютер;
- Кабель ЛВС. Сегмент кабеля ЛВС представляет собой отрезок кабеля типа экранированная витая пара 5-й категории не более 100 метров, снабженный с обоих концов разъемами типа RJ-45;
- Источник бесперебойного питания. Источник бесперебойного питания должен обеспечивать при аварии системы электропитания работу подключенного оборудования от аккумуляторов на время, необходимое для запуска резервной энергосистемы (если таковая присутствует), либо достаточного для сохранения всех необходимых данных и безопасного завершения работы системы. Для данной цели источник бесперебойного питания должен удовлетворять следующим условиям: мощность не менее 600 Вт. Источник бесперебойного питания не является обязательным для обеспечения функционирования ОС.

1.3. Перечень поддерживаемого оборудования

Перечень оборудования, поддерживаемого ОС «Циркон 37С»:

1. Процессоры:

Модель	Архитектура
Intel Core i3 Intel Core i5 Intel Core i7 Intel Xeon	Nehalem SandyBridge IvyBridge Haswell Broadwell Skylake
AMD Phenom II AMD Athlon II AMD Opteron	K10 K10.5
AMD Ryzen	Zen

2. Видеокарты:

- Matrox MGA G200e;
- ASPEED Graphics Family.

3. Звуковые карты:

- 7 Series/C216 Chipset Family High Definition Audio Controller;
- Realtek ALC887;
- 82801JI (ICH10 Family) HD Audio Controller.

4. Контроллеры сетевые:

- Intel i350 Gigabit Ethernet;
- Intel i210 Gigabit Ethernet;
- Intel 82574L Gigabit Ethernet;
- Realtek R8169;
- Realtek R8139;
- Realtek RTL8111/8168/8411 PCI Express Gigabit Ethernet;
- Realted RTL8111/8168B PCI Express Gigabit Ethernet;

- Realtek RTL8111H;
- Intel I219-LM Ethernet.

5. Контроллеры дисковые:
   - Intel Corporation C610/X99;
   - Intel Corporation C600/X79;
   - LSI Logic MegaRAID Tri-Mode SAS3508;
   - LSI Logic MegaRAID SAS-3 3108;
   - LSI Logic / Symbios Logic MegaRAID SAS-3 3008;
   - LSI Logic / Symbios Logic MegaRAID Tri-Mode SAS3408;
   - Intel Corporation C600/X79 series chipset SATA RAID Controller.

6. Принтеры:
   - с поддержкой PostScript;
   - с поддержкой PCL.

2. Описание типового варианта применения ОС «Циркон 37С»

В состав типовой схемы развертывания ПО АСТД 37С входят следующие аппаратные компоненты, объединенные в единую локально-вычислительную сеть:

1. Терминальный сервер – обеспечивающий работу терминальных сессий пользователей и представляющий пользовательский интерфейс для доступа к пользовательским интерфейсам общего программного обеспечения (ОПО) и специального программного обеспечения (СПО);

2. Сервер приложений – обеспечивающий работу серверных компонент ОПО и СПО;

3. Сервер резервного копирования – обеспечивающий возможность надежного восстановления данных;

4. АРМ администратора – обеспечивающее возможность подготовки к развертыванию виртуальных машин под управлением ОС «Циркон 37С», управление пользователями и установкой ОПО и СПО на виртуальные машины терминального сервера и сервера приложений;

5. АРМ на базе тонкого клиента, обеспечивающее возможность доступа пользователей к графическому интерфейсу ОС «Циркон 37С».

3. Установка ОС «Циркон 37С»

3.1. Начальные требования

В общем случае (например, для реализации типового варианта применения) при развертывании ОС «Циркон 37С» должны быть выполнены следующие шаги:

1. Подготовка АРМ администратора, включая установку ОС «Циркон 37С», инициализацию и настройку;
2. Развертывание ОС «Циркон 37С» на серверных платформах;
3. Формирование доменной структуры;
4. Создание виртуальной инфраструктуры.

3.2. Подготовка АРМ администратора

Программа установки

Программа установки ОС «Циркон 37С» состоит из нескольких компонент. Каждая компонента выполняет определенную задачу, осуществляя взаимодействие с пользователем через диалоговые окна, появляющиеся на определенных этапах работы программы установки.

В процессе установки на экране монитора появляются диалоговые окна, в которых могут содержаться: меню, списки полей, указания выполнить какие-либо действия или приглашения ответить на вопросы, предупреждения или информационные сообщения.

Переключение между элементами диалогового окна (меню, кнопки, поля ввода) осуществляется с помощью клавиши <Tab>. Выбор пункта меню осуществляется путем перемещения к нему курсора с помощью клавиш со стрелками вверх <↑> и вниз <↓>.

Существует два типа списков полей: кнопки с независимой фиксацией и кнопки с зависимой фиксацией. В первом случае для обозначения используются квадратные скобки, в которых при выделении появляется звездочка [*]. Во втором случае используются круглые скобки (*).

В списке полей первого типа возможно выбрать несколько пунктов одновременно («многие из многих»). В списке полей второго типа выбирается только один пункт («один из многих»). Выбор пункта в обоих случаях осуществляется нажатием клавиши <Пробел>.

При появлении предупреждений необходимо внимательно с ними ознакомиться и учесть в процессе установки. При появлении информационных сообщений никаких действий предпринимать не требуется. Как правило, информационные сообщения указывают на выполняемые операции этапов процесса установки.

Выбор метода установки

Для установки ОС «Циркон 37С» необходимо выбрать устройство чтения оптических дисков в качестве приоритетного.

В общем случае базовая операционная система (BIOS или UEFI) при включении компьютера выводит на экран сообщение вида «press F12 for boot menu» (на разных аппаратных платформах клавиша вызова меню может отличаться от указанной в примере), указывая пользователю способ вызова меню начальной загрузки.

Примечание. *Перед установкой ОС «Циркон 37С» необходимо отключить в настройках BIOS параметры «fast boot» и «secure boot»*.

После загрузки программы установки с дистрибутива ОС «Циркон 37С» пользователю будет предложено выбрать метод установки (рис. 1).

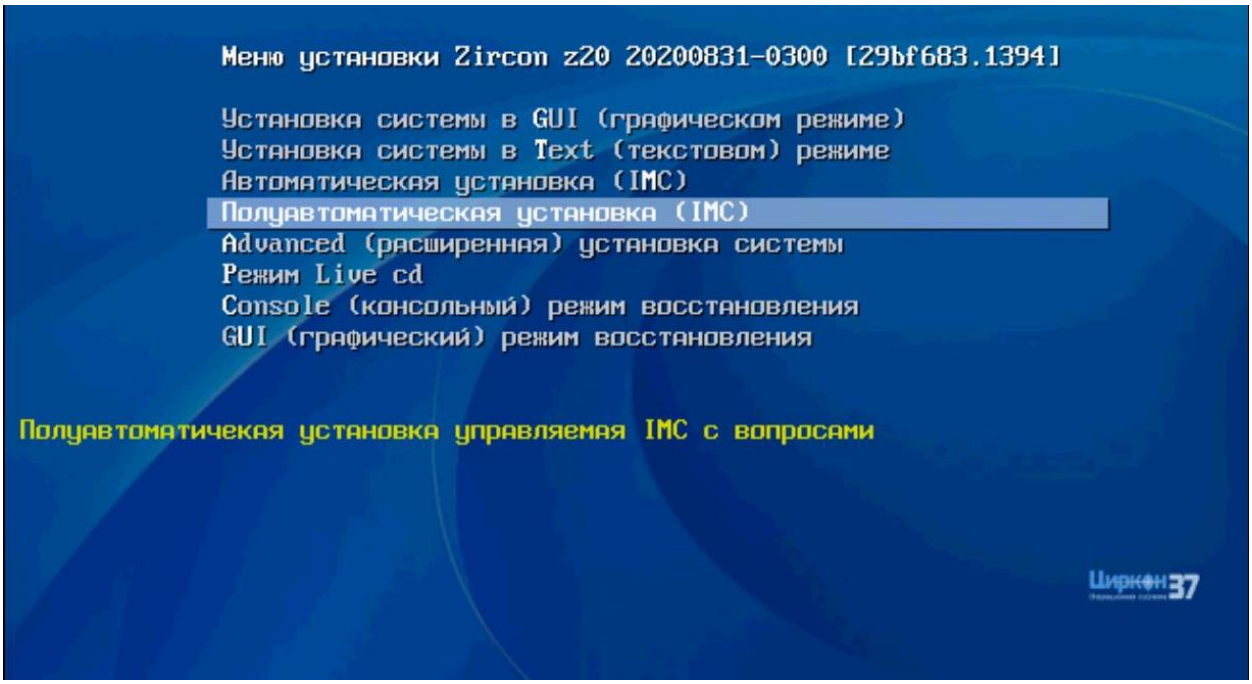

Рис. 1 – Выбор метода установки

По умолчанию пользователю рекомендуется автоматизированный метод установки.

В этом режиме компоненты автоматически запускаются в определенной разработчиком последовательности. Настройка учетной записи администратора. От выбора метода зависит количество параметров, которые будет необходимо

указывать вручную. В общем случае значение по умолчанию является оптимальным.

После выбора метода установки, программа установки ОС «Циркон 37С» осуществляет загрузку необходимого программного обеспечения (рис. 2).

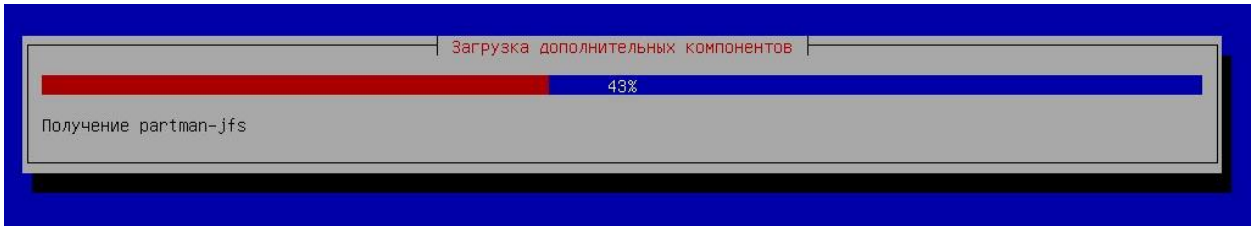

Рис. 2 – Установка дополнительных компонентов

Далее пользователю необходимо указать NETBIOS-имя АРМ, для которого осуществляется установка. После указания имени, необходимо нажать кнопку «Продолжить» (рис. 3).

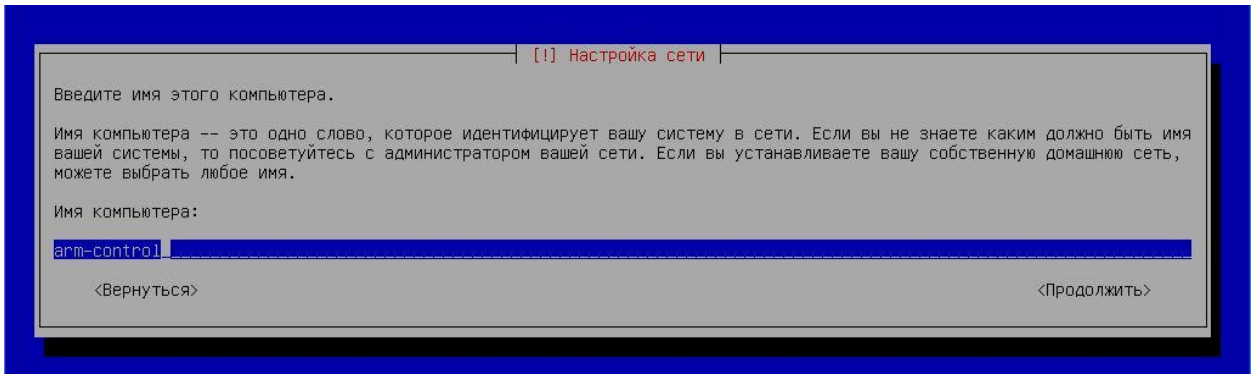

Рис. 3 – Присвоение имени АРМ

Создание учетной записи администратора

На следующем шаге необходимо указать пароль доступа для учетной записи администратора. По умолчанию в ОС «Циркон 37С» заблокирована учетная запись суперпользователя (учетная запись root), в качестве учетной записи администратора используется учетная запись secadmin (рис. 4).

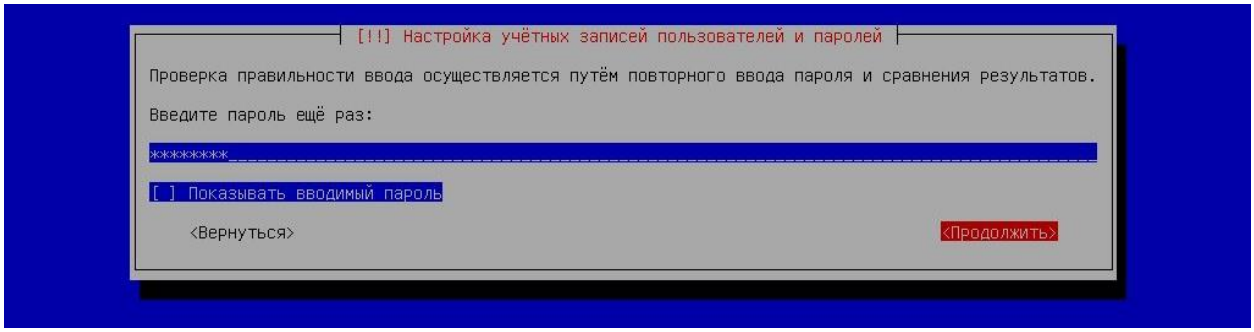

Рис. 4 – Настройка учетной записи secadmin

Пароль должен содержать хотя бы 1 символ из следующих категорий:

– прописные буквы латинского алфавита (A – Z);

– строчные буквы латинского алфавита (a – z);

– цифры (0 – 9);

– не алфавитно-цифровые символы (специальные символы) (например, «!», «$», «# » и т.п.).

Разметка логических томов на НЖМД

После установки пароля учетной записи администратора программа установки ОС «Циркон 37С» предложит пользователю произвести разметку подключенных к системе НЖМД, создать файловые системы на выбранных разделах и назначить им точки монтирования.

В диалоговом окне, представленном на рис. 5, пользователю предлагается выбрать метод создания разделов на НЖМД.

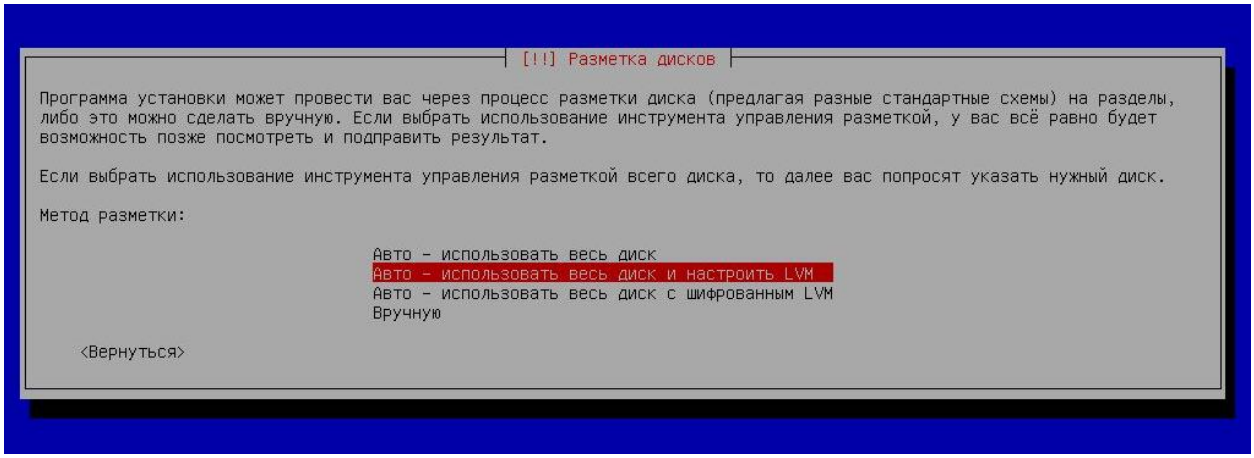

Рис. 5 – Выбор метода создания разделов на НЖМД

В общем случае наиболее оптимальным решением является создание логического тома, использующего все доступное на диске пространство (на рис. 5 пункт «Авто – использовать весь диск и настроить LVM»).

При создании разделов на жестком диске ОС «Циркон 37С» позволяет создавать как классические LVM разделы, так и разделы с использованием шифрования. LVM раздел представляет собой группу томов, объединенных внутри одного большого раздела, что позволяет изменять параметры входящих в него логических разделов без необходимости удаления данных.

При использовании LVM с шифрованием раздел (объединяющий группу томов) будет недоступен без специальной ключевой фразы, предоставляя тем самым дополнительную безопасность данным.

ОС «Циркон 37С» так же поддерживает различные виды расширенных настроек и использование устройств хранения, в частности:

- управление логическими томами (LVM);
- программный RAID (Поддерживается RAID 0, 1, 4, 5, 6 и 10 уровня);
- шифрование;
- serial ATA RAID (с помощью dmraid).

Примечание. *ОС «Циркон 37С» поддерживает следующие файловые системы для блочных устройств с возможностью хранения мандатного контекста: ext2, ext3, jfs, xfs, ext4 (используется в качестве файловой системы по умолчанию). При установке системы и хранении данных с использованием мандатного контекста следует выбирать из представленного списка файловых систем*.

После выбора метода создания разделов, пользователю предлагается выбрать диск, на котором будет осуществляться разметка разделов (рис. 6).

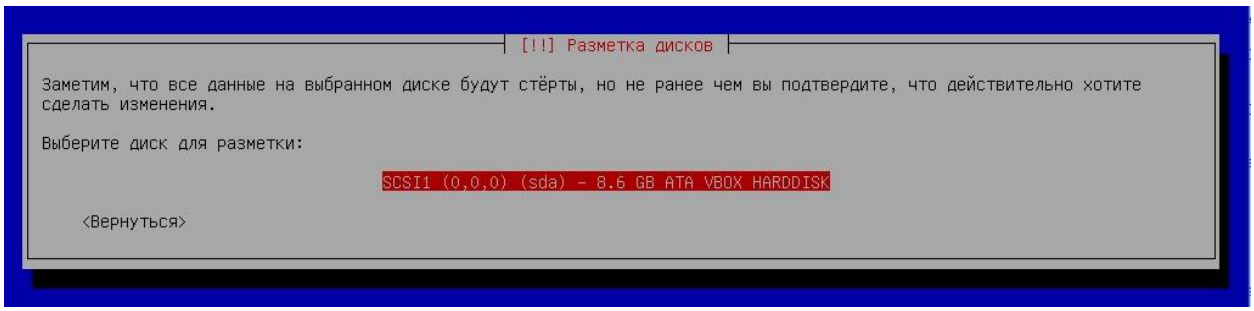

Рис. 6 – Выбор диска для разметки разделов

Далее необходимо задать схему разметки логических разделов и указать точки монтирования (рис. 7).

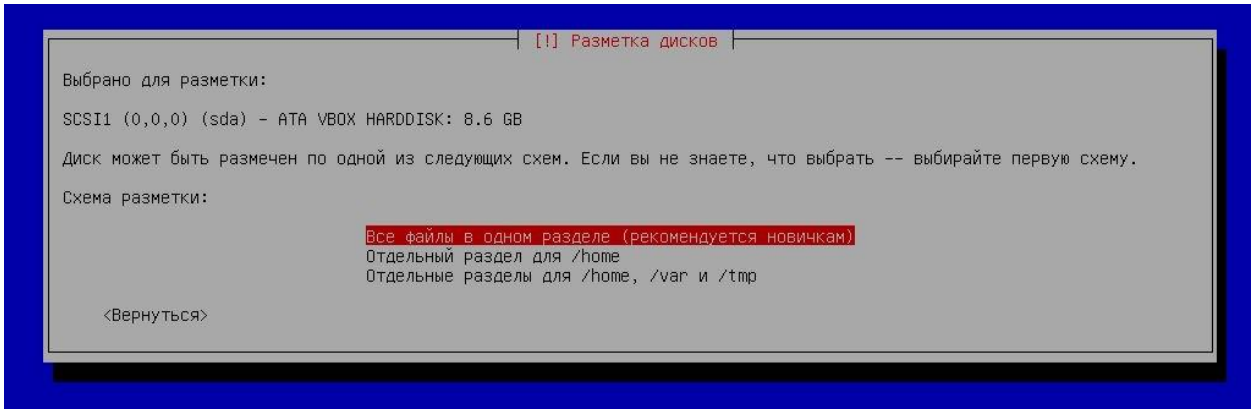

Рис. 7 – Выбор схемы разметки

Необходимо учитывать, что для работы корневого раздела требуется минимум один гигабайт свободного места. Если не учесть данное требование, то процесс разметки завершится ошибкой.

В общем случае наиболее оптимальным решением является использование схемы «Все файлы в одном разделе».

Примечание. *Если на этапе выбора метода создания разделов (см. рис. 5) на НЖМД был выбран метод «Авто – использовать весь диск с шифрованием и настроить LVM» была выбрана направляющая разметка с использованием LVM (с шифрованием), то программа установки создаст отдельный нешифрованных раздел «/boot». Остальные разделы, включая раздел подкачки, будут созданы внутри LVM*.

В последнем диалоговом окне пользователю будет предложено сохранить внесенные изменения (рис. 8). Для продолжения установки необходимо нажать кнопку «Да».

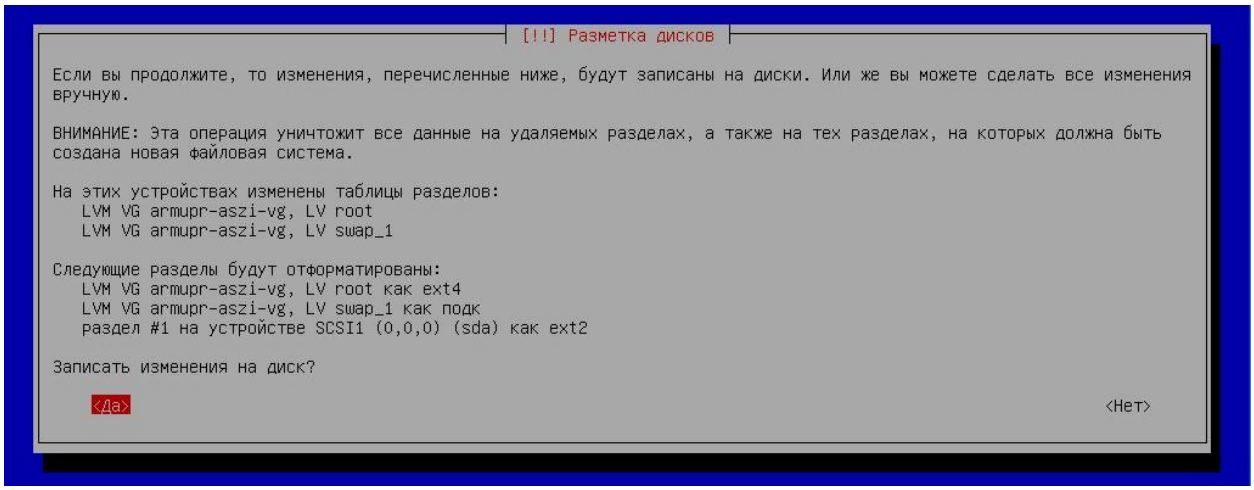

Рис. 8 – Сохранение внесенных изменений

После установки необходимых для функционирования ОС пакетов, необходимо выбрать устройство для установки загрузчика (рис. 9).

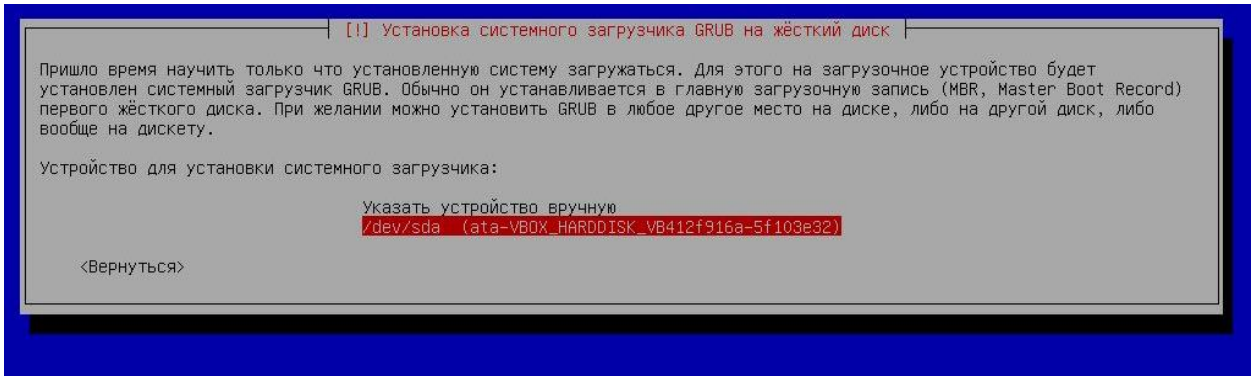

Рис. 9 – Установка загрузчика

Установка ОС «Циркон 37С» завершена (рис. 10).

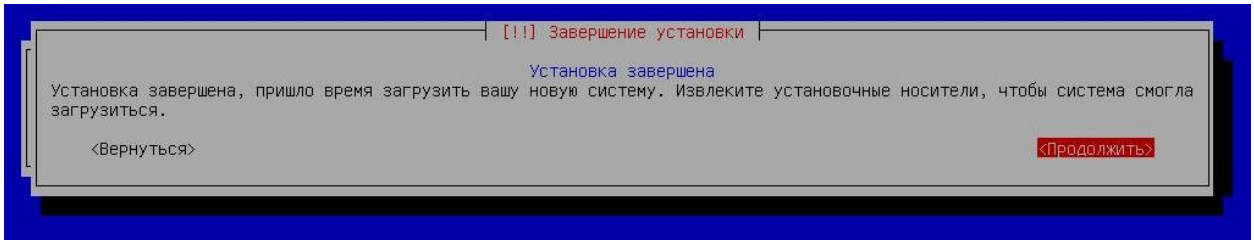

Рис. 10 – Окончание установки

Конфигурирование АРМ Администратора

После установки ОС «Циркон 37С» на АРМ администратора необходимо инициализировать роли управления для создания доменной структуры локальной сети:

1. Авторизоваться от имени пользователя secadmin.

2. Инициализировать роль управления:

```
sudo /opt/swemel/imc/bin/imcctl --configure-arm
```

3. В появившемся окне подтвердить необходимость установки программного обеспечения на АРМ администратора (рис. 11).

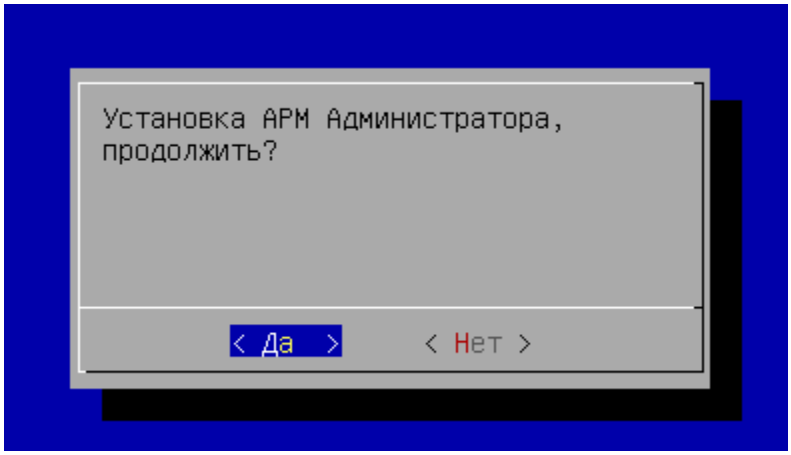

Рис. 11 – Диалоговое окно подтверждения установки

4. Указать NetBios имя АРМ администратора (рис. 12).

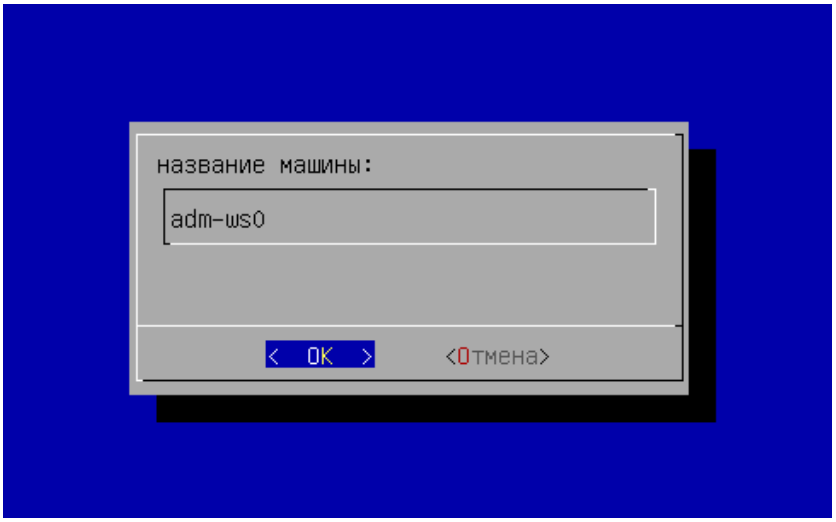

Рис. 12 – Указание имени АРМ

5. Задать пароль оператора (пароль будет использоваться для развертывания ПО на подчиненных узлах), в появившемся окне необходимо нажать «Да» для автоматической генерации пароля или «Нет» для задания пароля вручную (рис. 13).

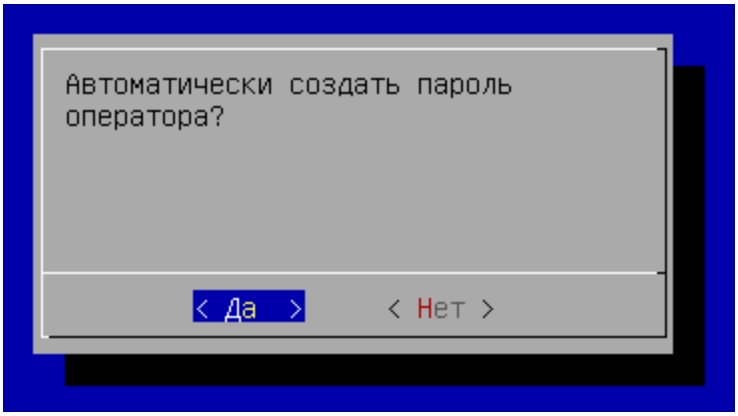

Рис. 13 – Создание пароля для оператора

6. Настроить сеть управления (рис. 14).

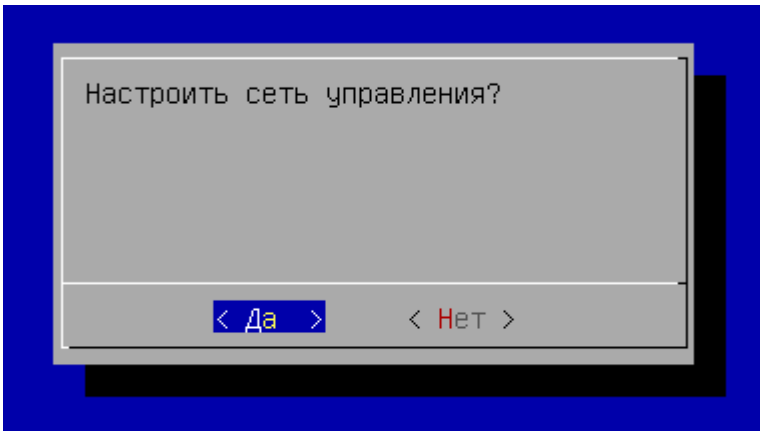

Рис. 14 – Настройка сети управления

7. Выбрать интерфейс, для которого будут сгенерированы псевдонимы для управления доменной структурой (рис. 15).

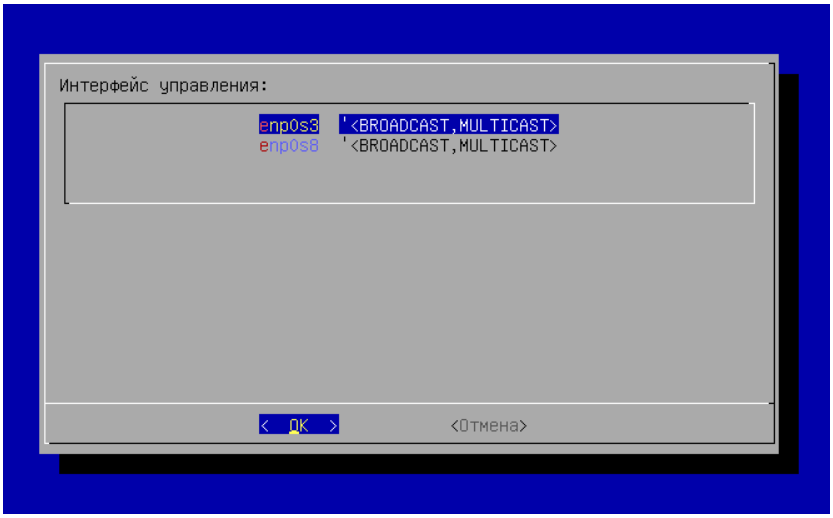

Рис. 15 – Выбор интерфейса управления

8. Указать IP-адрес и сетевую маску.

9. Указать путь образу дистрибутива ОС «Циркон 37С», например, к специальному файлу устройства чтения оптических дисков (рис. 16).

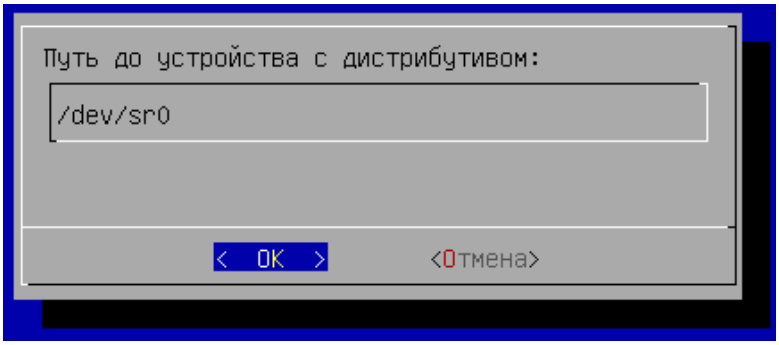

Рис. 16 – Задание пути к дистрибутиву

10. После завершения настройки перейти в графический режим (рис. 17).

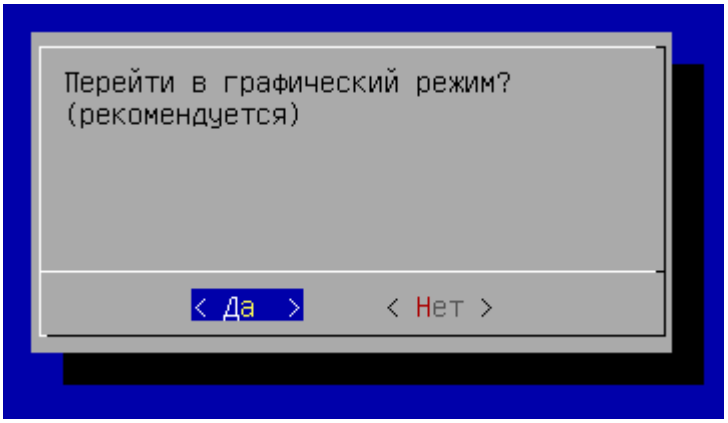

Рис. 17 – Переход в графический режим

11. Авторизоваться от имени пользователя operator (рис. 18).

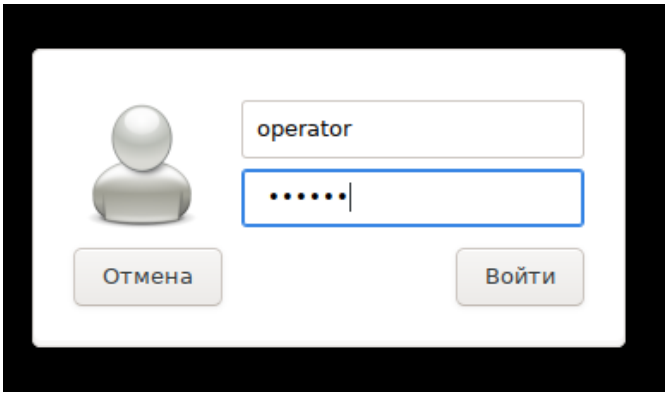

Рис. 18 – Окно авторизации

12. Запустить терминальную консоль MATE (рис. 19).

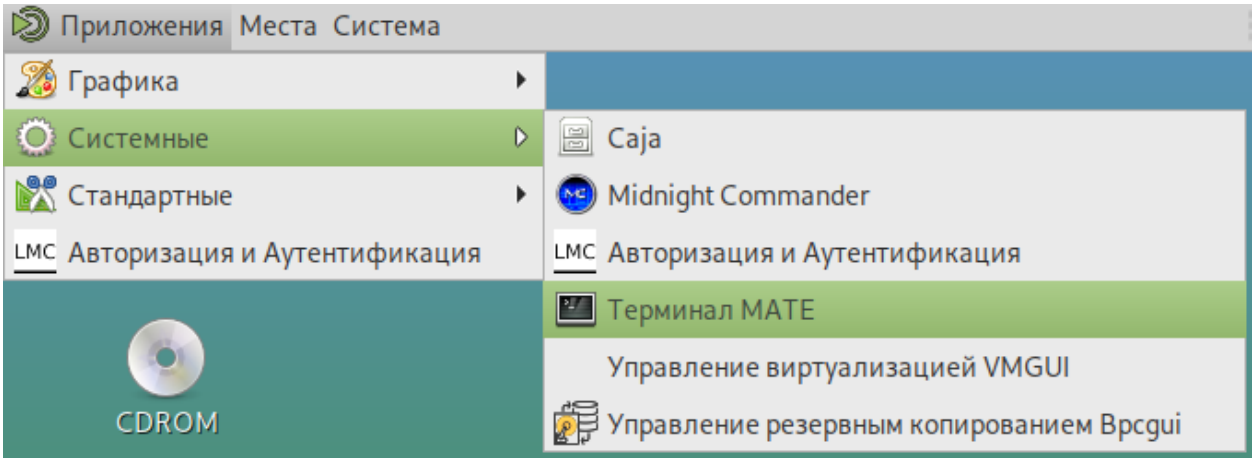

Рис. 19 – Выбор терминальной консоли MATE

13. Сгенерировать конфигурационные файлы (файлы-inventory) (рис. 20).

```
imcctl --configure-inventory
```

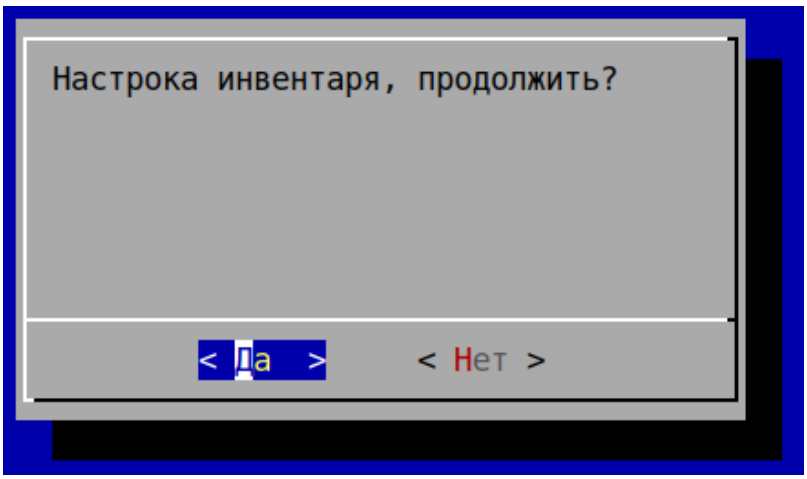

Рис. 20 – Диалоговое окно генерации конфигурационных файлов

14. Сгенерировать пароли доступа к сетевой инфраструктуре автоматически или использовать ручной ввод (для ручного ввода необходимо выбрать «Нет») (рис. 21).

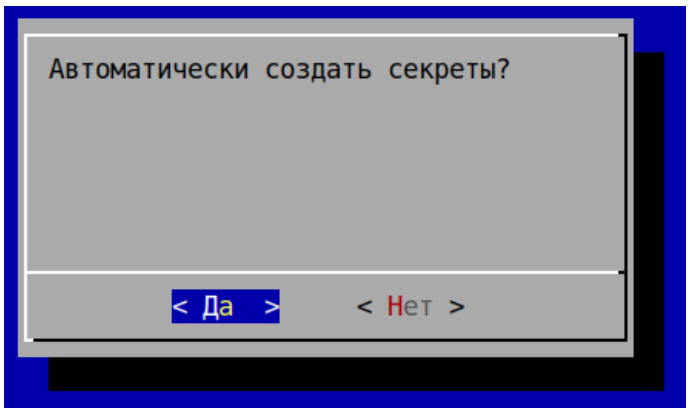

Рис. 21 – Диалоговое окно генерации паролей

15. Ввести название домена (рис. 22).

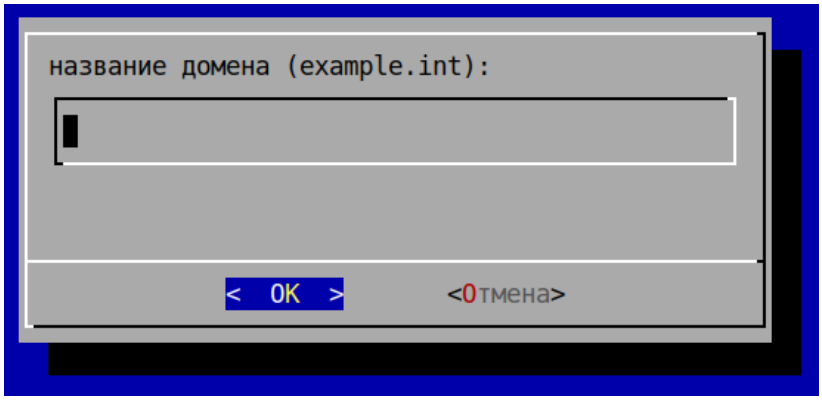

Рис. 22 – Указание имени домена

16. Задать пароль для ключевых файлов SSH (рис. 23).

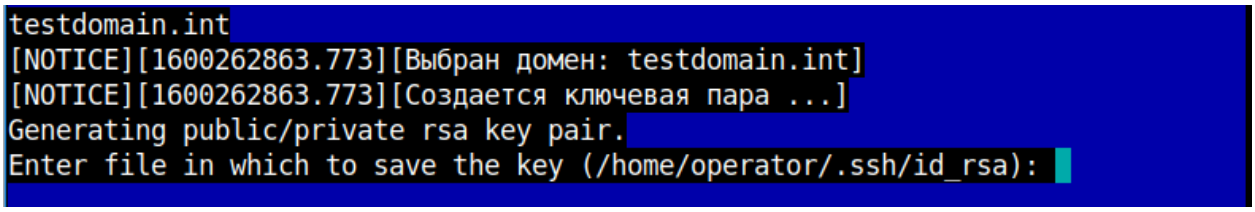

Рис. 23 – Задание пароля для ключевых файлов SSH

17. После завершения генерации конфигурационных файлов (рис. 24) необходимо перезагрузить АРМ администратора и авторизоваться от имени пользователя operator.

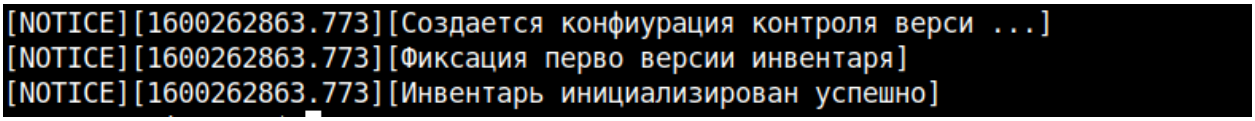

Рис. 24 – Окончание генерации конфигурационных файлов

18. Применить роль узла администрирования для АРМ администратора:

```
cd ~/imc
NewOrder --limit=adm-ws0 --roles=NodePrepare --ask-password
```

19. Авторизоваться от имени пользователя secadmin и установить утилиту для управления картой меток.

```
su secadmin
sudo apt-get install lme
```

20. Перевести АРМ администратора из сервисного режима работы (ServiceMode) в рабочий режим работы (ProductionMode).

```
su operator
NewOrder --roles=ProductionMode --limit=adm-ws0
```

Примечание. *Выполнение данной команды блокирует возможность изменения в среде выполнения АРМ администратора в т. ч., блокируется возможность выполнения привилегированных команд (например, через sudo)*.

21. АРМ администратора развернут и готов к работе.

3.3. Развертывание доменной структуры

Подготовка структуры

Для развертывания и управления виртуальными машинами необходимо описать структуру создаваемой сети. Для этого необходимо отредактировать конфигурационные файлы, размещенные в каталоге /home/operator/imc.

Каталог имеет следующую структуру:

- ansible.cfg: конфигурационный файл средства настройки и развертывания инфраструктуры;
- каталог data содержит данные собираемые в процессе функционирования системы (например, системные конфигурации объекта управления (ОУ));
- каталог etc, содержит корневой сертификат, а также, сертификаты на ОУ, карту меток и т.п.;
- каталог group_vars содержит переменные групп специфичные для каждой отдельной группы ОУ;
- каталог host_vars содержит переменные специфичные для каждого отдельного ОУ;
- каталог roles корневой каталог, содержащий конфигурационные файлы для различных ролей ОУ;
- конфигурационный файл <DOMAINNAME>.yml, содержит сведения о структуре домена (название файла соответствует названию домена, указанному при развертывании).

Перед началом развертывания защищенной инфраструктуры необходимо сформировать карту меток и сконфигурировать инвентарь.

Создание карты мандатных меток

Концепция фильтрации сетевого потока

При создании карты меток необходимо придерживаться концепции фильтрации сетевого потока виртуальной инфраструктуры заложенной в ПО АСТД 37С.

Данный принцип предполагает следующие состояния меток:

1. Строгое доминирование – набор атрибутов метки 1 доминирует над меткой 2 – в случае если уровень конфиденциальности метки 1 больше или равен уровню конфиденциальности метки 2, а набор категорий метки 2 является подмножеством набора категорий метки 1.

   Исключения составляют случаи, при которых метки имеют идентичный уровень конфиденциальности и набор категорий.
2. Равенство – набор атрибутов метки 1 равен набору атрибутов метки 2 – в случае если метки имеют идентичный уровень конфиденциальности и набор категорий.
3. Доминирование – набор атрибутов метки 1 доминирует над меткой 2 · в случае если уровень конфиденциальности метки 1 больше или равен уровню конфиденциальности метки 2, а набор категорий метки 2 является подмножеством набора категорий метки 1.
4. Несравнимость – наборы атрибутов меток 1 и 2 являются несравнимыми в случае если ни одна из меток не доминирует над другой.

Состав атрибутов информационной метки

DOI – идентификатор домена интерпретации – положительное целое число длиной 32 бит, его значение определяет независимо администрируемые пространства мандатных меток. Метки с отличающимся идентификатором домена интерпретации, но идентичные во всем остальном, считаются не пересекающимися (несравнимыми) между собой.

Диапазон атрибутов меток, характеризующий минимальный и максимальный уровень доступа.

unaware (только для однометочных, объектов L ≡ H) ▪ атрибут указывающий на отсутствие требования к наличию cipso для указанного субъекта, информация о принадлежности субъекта определенной метке берется из конфигурации гипервизора.

mlp – multilevel ports (только для зон) ▪ это перечни udp, tcp и sctp портов, для которых предполагается multilevel трафик.

ПО АСТД 37С допускает *multilevel* трафик зон, только если он исходит из *mlp*. Весь остальной исходящий трафик обрабатывается так, как будто объект однометочный с меткой H.

Правила фильтрации сетевого потока виртуальной инфраструктуры

В ПО АСТД 37С можно выделить следующие субъекты виртуальной инфраструктуры:

- Сеть – подсеть IPv4, помеченная как имеющая информационную метку.
- Зона – сетевой интерфейс, помеченный как имеющий информационную метку. За сетевым интерфейсом предполагается наличие виртуальной машины.

При разграничении доступа необходимо придерживаться следующих положений:

1. Фильтрация виртуальной инфраструктуры затрагивает сетевой поток, направленный из зоны в зону, либо из зоны в сеть и наоборот.
2. При определении метки сетевого потока зона имеет больший приоритет перед сетью.
3. При определении метки сетевого потока сеть меньшего размера (с более длинной маской) имеет приоритет над сетью большего размера (с более короткой маской).

4. Если зона или сеть оперирует только однометочной информацией, то ПО АСТД 37С позволяет задать ему атрибут unaware, при этом пакету не назначается метка.
5. Если атрибут unaware не установлен, ПО АСТД 37С будет обрабатывать пакет только в случае корректно назначенной метки.
6. Если для сети указан диапазон меток, то из такой сети могут выходить пакеты, только если метка пакет условию метки узла назначения.

Утилита генерации карты

Создание карты меток осуществляется на АРМ администратора с помощью графического интерфейса LME (рис. 25).

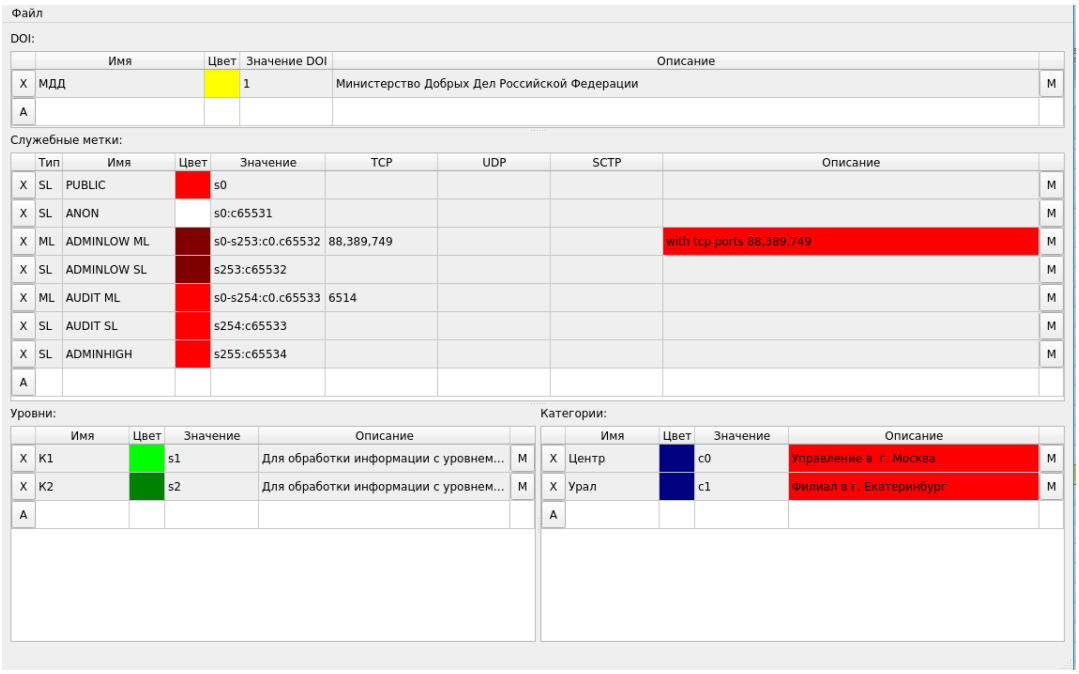

Рис. 25 – Интерфейс LME

В поле «DOI» необходимо указать произвольный идентификатор домена.

В разделе «Служебные метки» необходимо указать набор меток, которые будут использоваться в информационной системе. Согласно правилам фильтрации сетевого трафика метки могут быть следующих типов:

- multilevel (многометочный – ML);
- singlelevel (однометочный – SL).

У многометочного домена необходимо указать набор портов, на которые будет осуществляться передача информации.

В разделе уровни необходимо указать уровни обрабатываемой в автоматизированной системе информации.

В разделе категории необходимо указать категории информации для разграничения доступа в рамках одного уровня.

После заполнения всех полей необходимо сохранить внесенные изменения.

Настройка инвентаря

Работа с инвентарем осуществляется с помощью интерфейса *imc*.

Все операции должны осуществляться под пользователем *operator*.

Объекты управления добавляются в файл DOMAINNAME.yml, расположенный в корне *imcroot* (как правило, /home/operator/imc), например:

```
all:
  hosts:
    adm-ws0:
  children:
    hv:
    nodes:
    zm:
    kerberos:
    ldap:
    d_members:
    admin:
      hosts:
        adm-ws0:
```

АРМ Администратора (adm-ws0) является членом группы admin и группы all.

- all – специальная группа, в которой должны быть перечислены все объекты системы;
- hv – группа, содержащая ОУ выполняющие функции гипервизоров. В эту группу объекты добавляются автоматически при развертывании ролей связанных с виртуализацией;

- nodes – типовая группа для машин, не выполняющих функции виртуализации;
- zm – машины, выполняющие функции зонного менеджера;
- kerberos – машины выполняющие функции контроллеров домена;
- ldap – группа ldap-серверов;
- d_members – содержит список всех членов домена;
- admin – АРМ выполняющие функции АРМ Администратора.

Переменные для объектов хранятся в файлах *host_vars/hostname/vars.yml*:

```
operator@auto:~/imc$ cat host_vars/node1.yml
ansible_host: 192.168.250.33
```

Закрытые для просмотра переменные для объектов (если есть), хранятся в файлах *host_vars/hostname/vault.yml*.

Для создания закрытого хранилища хоста следует выполнить команду:

```
ansible-vault create host_vars/hostname/vault.yml
```

после чего ввести пароль на создаваемое хранилище.

Операцию по добавлению хоста в инвентарь можно производить как вручную, путем редактирования файла инвентаря и файлов хранилищ переменных так и автоматически выполнив команду:

```
NewOrder --roles=Host2Inventory --limit=<имя хоста арм управления> --extra-vars="hostname=<имя нового хоста> ipaddr=<ipv4  адрес управления нового хоста> netmask=<ipv4 маска адреса управления нового хоста>"
```

Либо, если для нового хоста для получения сетевого доступа требуется использовать определенную метку, выполняется следующее:

```
NewOrder --roles=Host2Inventory --limit=<имя хоста арм управления> --extra-vars="hostname=<имя нового хоста> ipaddr=<ipv4  адрес управления нового хоста> netmask=<ipv4 маска адреса управления нового хоста> smack_label=<метка smack используемая для подключения>"
```

Добавление нового объекта управления

Добавление нового объекта управления с помощью консольного интерфейса imc

Добавление нового объекта управления через консольный интерфейс imc осуществляется по следующим сценариям:

На целевой машине:

1. Установить систему в варианте «полуавтоматическая установка (IMC)»;

2. После загрузки машины, зарегистрироваться с правами secadmin и выполнить команду для задания адреса на интерфейсе управления и выбора применяемого шаблона настроек мандатного контроля доступа:

```
sudo /opt/swemel/imc/bin/configure_node --mac
```

На АРМ администратора (adm-ws0):

1. Объект управления должен быть добавлен в инвентарь;

2. Не обязательно:

   – добавить в /etc/hosts адрес и имя нового объекта управления;

   – добавить отпечаток нового объекта управления в базу отпечатков known_hosts:

```
operator@adm-ws0:~$ ssh secadmin@<ОУ>
```

3) Взять объект управления под управление командой:

```
$ NewOrder --limit=node1 --roles=NodePrepare --ask-password

SSH password:
SUDO password[defaults to SSH password]:
Vault password:

PLAY [Taking new node under control]
*****************************************************
...
```

Далее:

- На запрос SSH *password* указать пароль, указанный при установке объекта управления;
- Для SUDO – нажать клавишу <Enter>;
- Для vault – ввести пароль от хранилища.

После окончания отработки задач, пользователю secadmin будет назначен пароль, заданный при настройке инвентаря, а сам объект управления перезагружен (регулируется переменное *'prepare_restart: true' в group_vars/all*) и приведен в режим обслуживания.

В режиме обслуживания служебный пользователь imc имеет возможность выполнять sudo без ограничений и ввода пароля.

Проверить цепочку управления можно выполнив команду:

```
$ ansible -m shell -a 'id' node2

node2 | CHANGED | rc=0 >>
uid=555(imc) gid=555(imc) группы=555(imc)
```

Аналогично, должен работать вход *'ssh imc@node2'*.

Добавление нового объекта управления с помощью графического интерфейса imcgui

Добавление нового объекта управления с помощью графического интерфейса imcgui осуществляется по следующим сценариям:

На целевой машине:

1. Установить систему в варианте «Автоматическая установка (IMC)»;

2. После загрузки машины, зарегистрироваться с правами secadmin и выполнить команду для задания адреса на интерфейсе управления и выбора применяемого шаблона настроек мандатного контроля доступа:

```
sudo /opt/swemel/imc/bin/configure_node --mac
```

На АРМ администратора:

1. Перед добавлением нового объекта управления необходимо добавить в /etc/hosts адрес и имя нового объекта управления;

2. Для добавления нового объекта управления в инвентарь необходимо нажать на кнопку «H+». Будет открыто диалоговое окно «Добавить хост» (рис. 26).

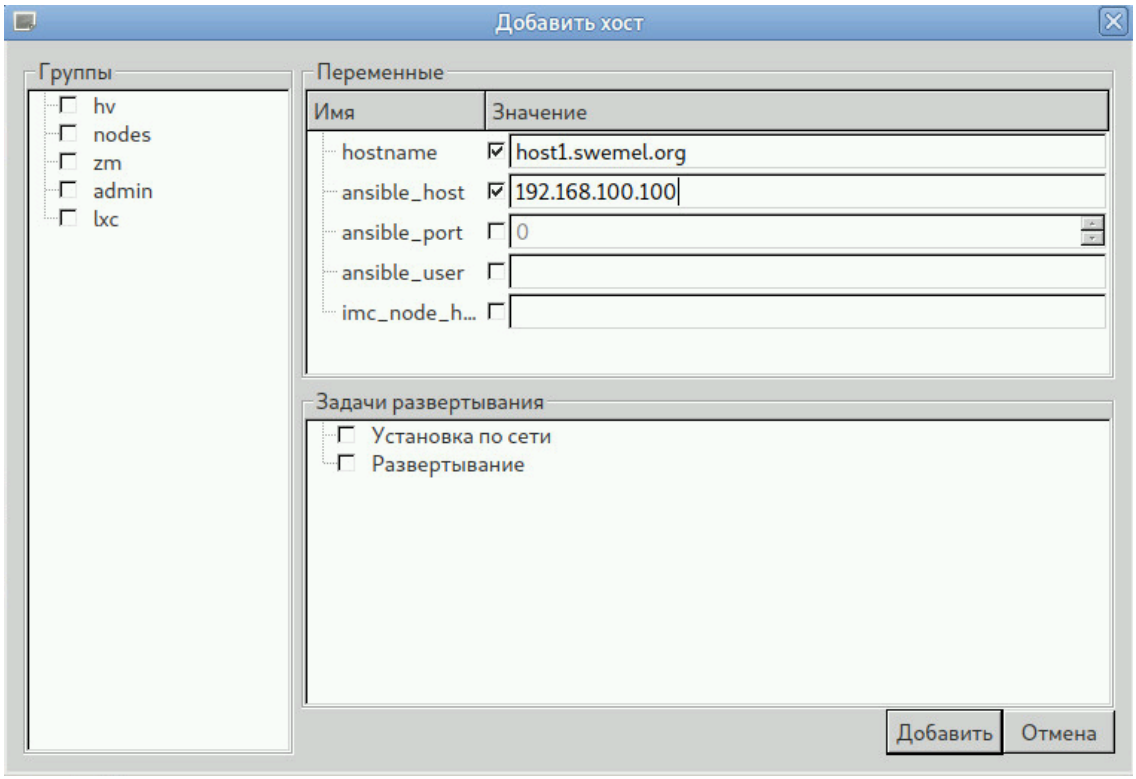

Рис. 26 – Диалоговое окно «Добавить хост»

3. Задать переменные hostname и ansible_host;

4. Отключить триггер «Развертывание»;

5. Нажать на кнопку ·Добавить·;

6. Добавить отпечаток нового объекта управления в базу отпечатков known_hosts:

```
secadmin@auto:~/imc$ ssh host1
The authenticity of host 'host1 (192.168.100.100)' can't be
established.
ECDSA key fingerprint is
SHA256:+DguERKo2JEAAT/PBg59elcn/bVa43miuXqcrnHvcu0.
Are you sure you want to continue connecting (yes/no)? yes
```

```
Warning: Permanently added 'host1,192.168.100.100' (ECDSA) to
the list of known hosts.
secadmin@host1's password:
```

7. Взять объект управления под управление. Для этого нажать на кнопку «Р», после чего будет открыт диалог «Новое задание» (рис. 27). Выбрать шаблон *pb_newobject.yml*, затем выбрать объект управления и нажать на кнопку [Запуск]. Дождаться завершения операции.

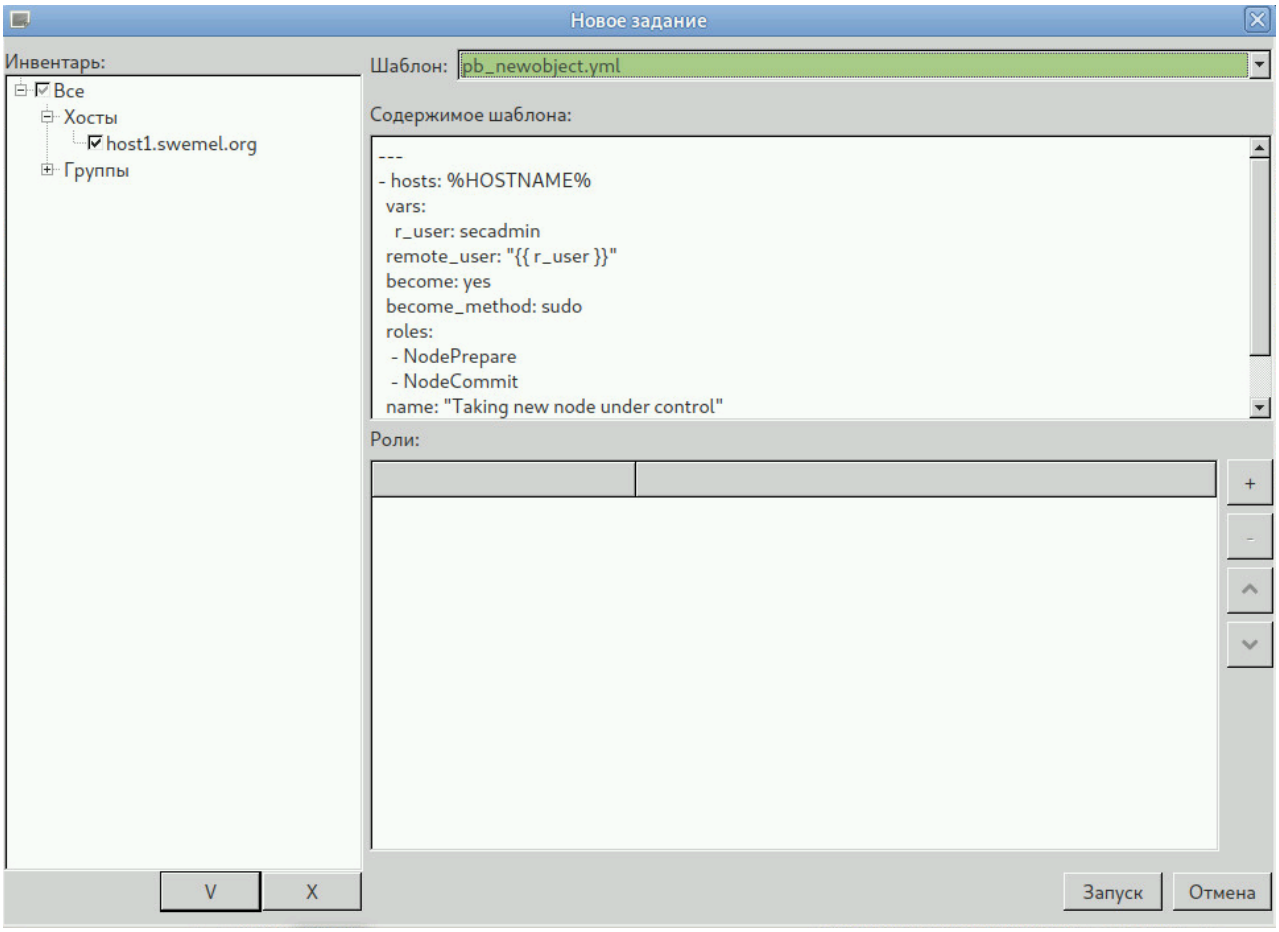

Рис. 27 – Добавление нового ОУ.
Диалоговое окно «Новое задание»

После окончания отработки задач, пользователю *secadmin* будет назначен пароль, заданный при настройке инвентаря, а сам объект управления перезагружен (регулируется переменная *'prepare_restart: true' в group_vars/all*) и приведен в режим обслуживания. В данном режиме служебный пользователь *imc* имеет возможность выполнять s*u*do без ограничений и ввода пароля. Проверить цепочку управления можно выполнив команду:

```
ansible -m shell -a 'id' host1 .
host1 | CHANGED | rc=0 >>
uid=555(imc) gid=555(imc) группы=555(imc)
```

Аналогично, должен работать вход 'ssh imc@host1'.

Применение ролей

В режиме обслуживания объект управления настраивается в соответствии со своими функциями путем применения цепочки ролей, приводящих его в заданное состояние.

Применение ролей с помощью консольного интерфейса imc

Для назначения объекту управления соответствующих функций, необходимо выполнить команду *NewOrder* с перечислением ролей.

Например, для настройки агрегатора системных журналов и записей аудита, необходимо добавить объект управления в группу *zm* (в этой группе перечисляются объекты управления, которые работают с несколькими метками).

```
file: swemel.org.yml
all:
  hosts:
    node1:
    node2:
  children:
    hv:
    nodes:
    zm:
      hosts:
        node2:
```

и выполнить следующую команду:

```
NewOrder --
roles='BasicAudit,AuditForward,ZoneManager,RsyslogCollector' --
limit=node2
```

которая:

- включит аудит выполняемых команд;
- включит копирование сообщений аудита в системный журнал;
- установит и настроит зонный менеджер, скопирует карту сетей и меток (etc/net.label и etc/map.label);
- настроит rsyslog в режиме приема сообщений на порту tcp/6514, создаст агрегированный файл журналов в /var/log/sb/full.log и настроит его ротацию с годовой архивацией.

Для добавления другого объекта управления как клиента для агрегатора журналов, необходимо выполнять следующую команду:

```
NewOrder --roles='BasicAudit,AuditForward,LogForward' --
limit=node1 --extra-vars='log_server_ip=10.1.140.120'
```

где 10.1.140.120 – ip адрес сервера-агрегатора node2, а роль LogForward включает копирование системного журнала на заданный адрес.

После этого в журнале /var/log/sb/full.log должны появятся копии записей из журнала node1.

Применение ролей с помощью графического интерфейса imcgui

Для назначения ОУ соответствующих функций, необходимо:

1. Нажать на кнопку «Р» в диалоговом окне «Новое задание» (рис. 28);

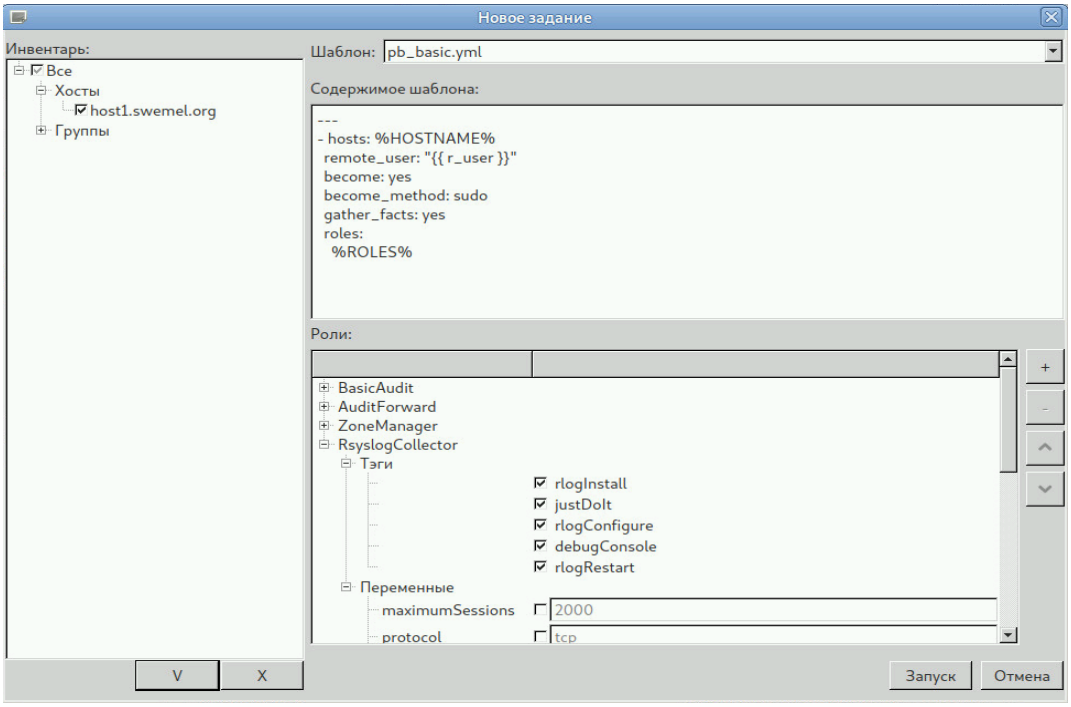

Рис. 28 – Применение ролей.
Диалоговое окно «Новое задание»

2. Выбрать шаблон pb_basic.yml;

3. Выбрать объекты управления, для которых будут применены роли;

4. Добавить роли, настроить переменные и выбрать необходимые тэги, после чего нажать на кнопку [Запуск].

При этом будут выполнены следующие действия:

- Включение аудита выполняемых команд;
- Включение копирования сообщений аудита в системный журнал;
- Установка и настройка зонного менеджера, копирование карты сетей и меток (etc/net.label и etc/map.label);
- Настройка rsyslog в режиме приема сообщений на порту tcp/6514, создание агрегированного файла журналов в /var/log/sb/full.log и настройка его ротации с годовой архивацией.

Для добавления другого объекта управления (host2.swemel.org) как клиента для агрегатора журналов, необходимо выбрать роли: BasicAudit, AuditForward, LogForward и для переменной *log_server_ip* задать значение 10.1.140.120.

Здесь 10.1.140.120 – ip адрес сервера-агрегатора host1.swemel.org, а роль LogForward – включает копирование системного журнала на заданный адрес. После этого в журнале /var/log/sb/full.log должны появиться копии записей из журнала host2.swemel.org.

Перевод в режим эксплуатации

После окончания настройки объекта управления, необходимо перевести объект управления в режим эксплуатации, в котором пользователь imc не имеет возможности вносить изменения в настройки ОС, а перечень привилегированных команд ограничен.

Для этого необходимо выполнить следующие действия в зависимости от способа работы с системой:

1. С помощью консольного интерфейса imc необходимо ввести команду:

```
NewOrder productionmode.yml --limit=HOSTNAME
```

где HOSTNAME – объект управления, для которого включается режим эксплуатации.

2. С помощью графического интерфейса imcgui необходимо:

- Выбрать объект управления в дереве;
- Вызвать контекстное меню;
- Выбрать команду «Перевод в режим эксплуатации».

Перевод в режим обслуживания

Для внесения изменений в конфигурационные файлы, перечень программного обеспечения и т.п., необходимо перевести объект управления в режим обслуживания. Для этого необходимо знать пароль пользователя secadmin, заданный при настройке инвентаря.

Перевод осуществляется в зависимости от способа работы с системой:

1. С помощью консольного интерфейса imc необходимо ввести команду:

```
NewOrder servicemode.yml --limit=HOSTNAME --ask-password
```

после чего пользователь imc вновь получает права администратора;

2. С помощью графического интерфейса imcgui необходимо:

- Выбрать объект управления в дереве;
- Вызвать контекстное меню;
- Выбрать команду «Перевод в режим обслуживания».

3.4. Развертывание виртуальной инфраструктуры

Назначение роли гипервизора

Для создания виртуальной инфраструктуры серверам, на которых планируется поднятие виртуальных машин, необходимо назначить роль гипервизора. Назначение роли осуществляется с АРМ администратора от имени пользователя operator следующей командой:

```
NewOrder --limit=<хост назначения> --roles=VirtWS
```

После выполнения роли для управления инфраструктурой можно воспользоваться утилитой virt-manager.

Графический интерфейс управления

Управление виртуальной инфраструктурой осуществляется с АРМ администратора от имени пользователя operator через графический интерфейс virt-manager.

Запуск графической утилиты управления virt-manager осуществляется командой:

```
operator@adm-ws0:~$ ssh imc@x.x.x.x -X virt-manager
```

где x.x.x.x – адрес установленного гипервизора.

Окно основного приложения представляет собой набор элементов управления (рис. 29).

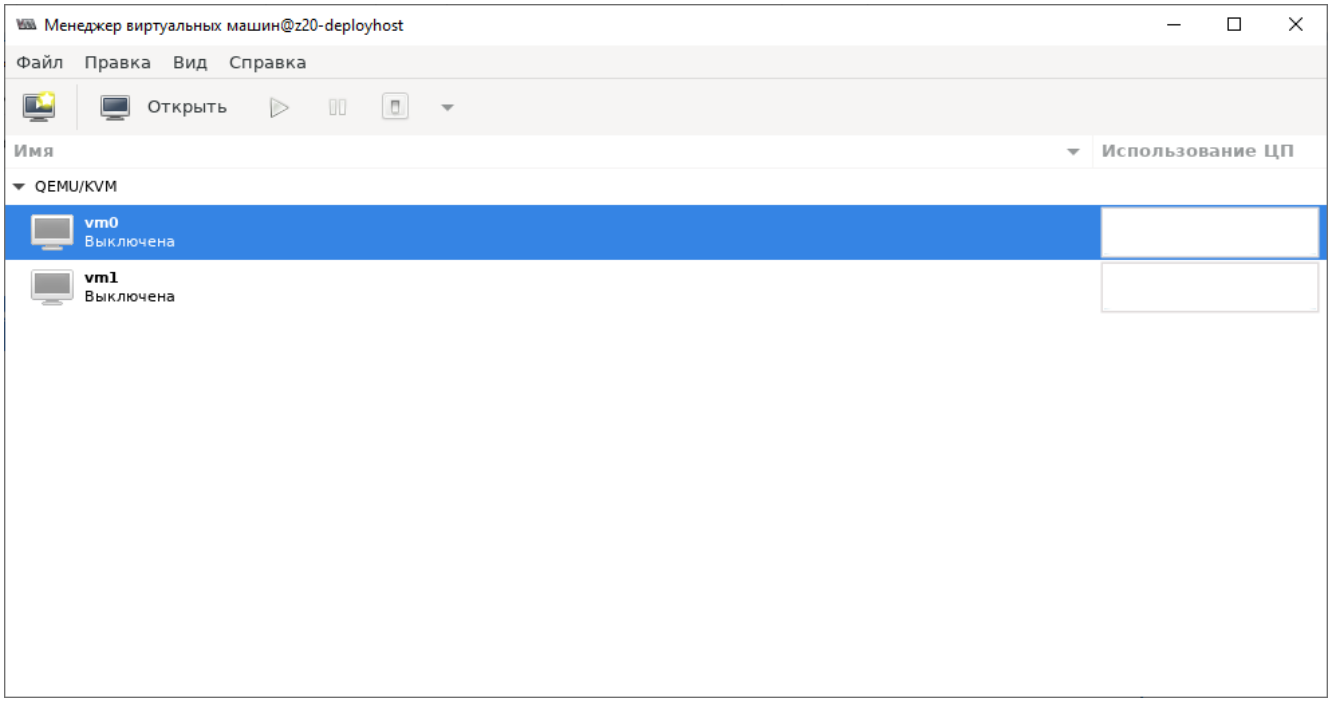

Рис. 29 – Интерфейс графической утилиты управления virt-manager

Метки безопасности

Метка виртуальной машины определяет возможный диапазон меток, который может быть использован виртуальными сетевыми адресами в указанной виртуальной машине.

Например, чтобы создать виртуальную машину с меткой «doi:1 mls:s8:c8» (рис. 30) необходимо выполнить следующие действия:

1. Выбрать элемент «Создать виртуальную машину» в меню Файл;

2. Сконфигурировать параметры виртуальной машины;

3. Указать метку виртуальной машины в завершающем диалоге создания виртуальной машины.

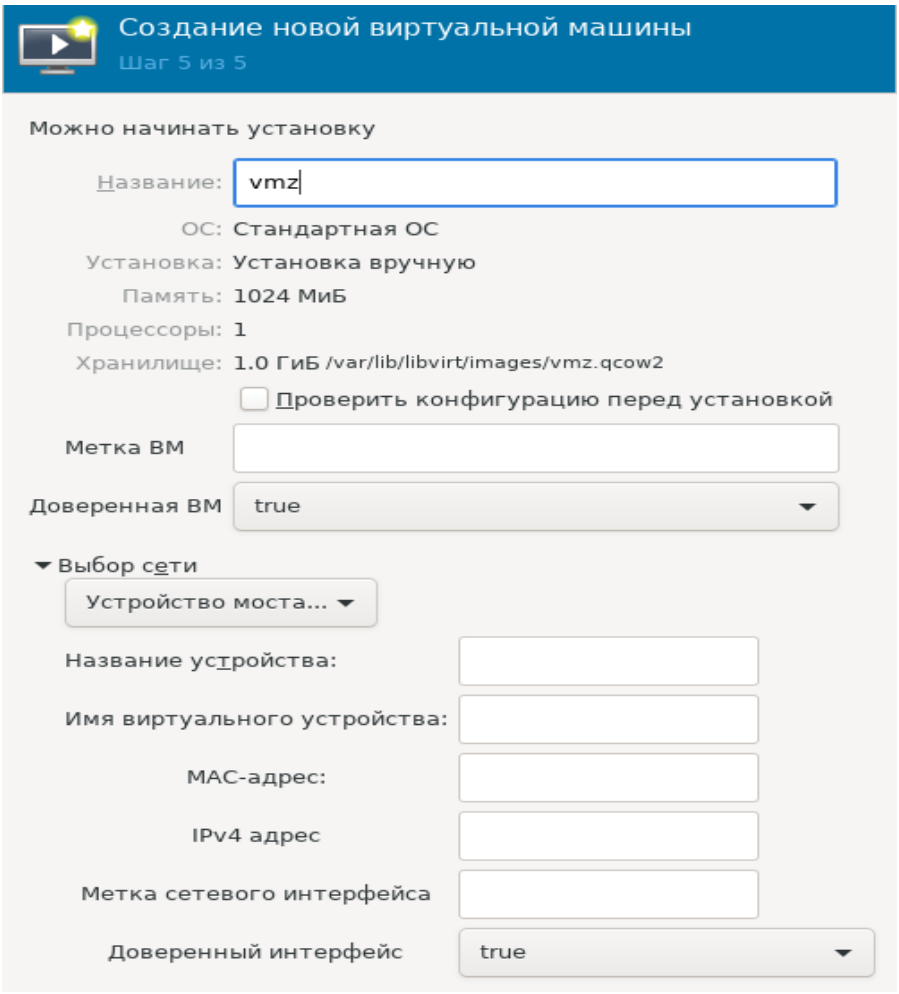

Рис. 30 – Назначение метки
виртуальной машине при создании

При установке параметра «Доверенная ВМ» во включенной состояние метка для виртуальной машины не влияет на правила фильтрации *zm*, в этом случае правила фильтрации *zm* на данную виртуальную машину не распространяются. В противном случае правила фильтрации принудительно создаются и метка виртуальной машины проверяется на совместимость с метками сетевых интерфейсов.

Метку виртуальной машины и параметр «Доверенная машина» можно изменить из окна редактирования виртуальной машины, как показано на рис. 31.

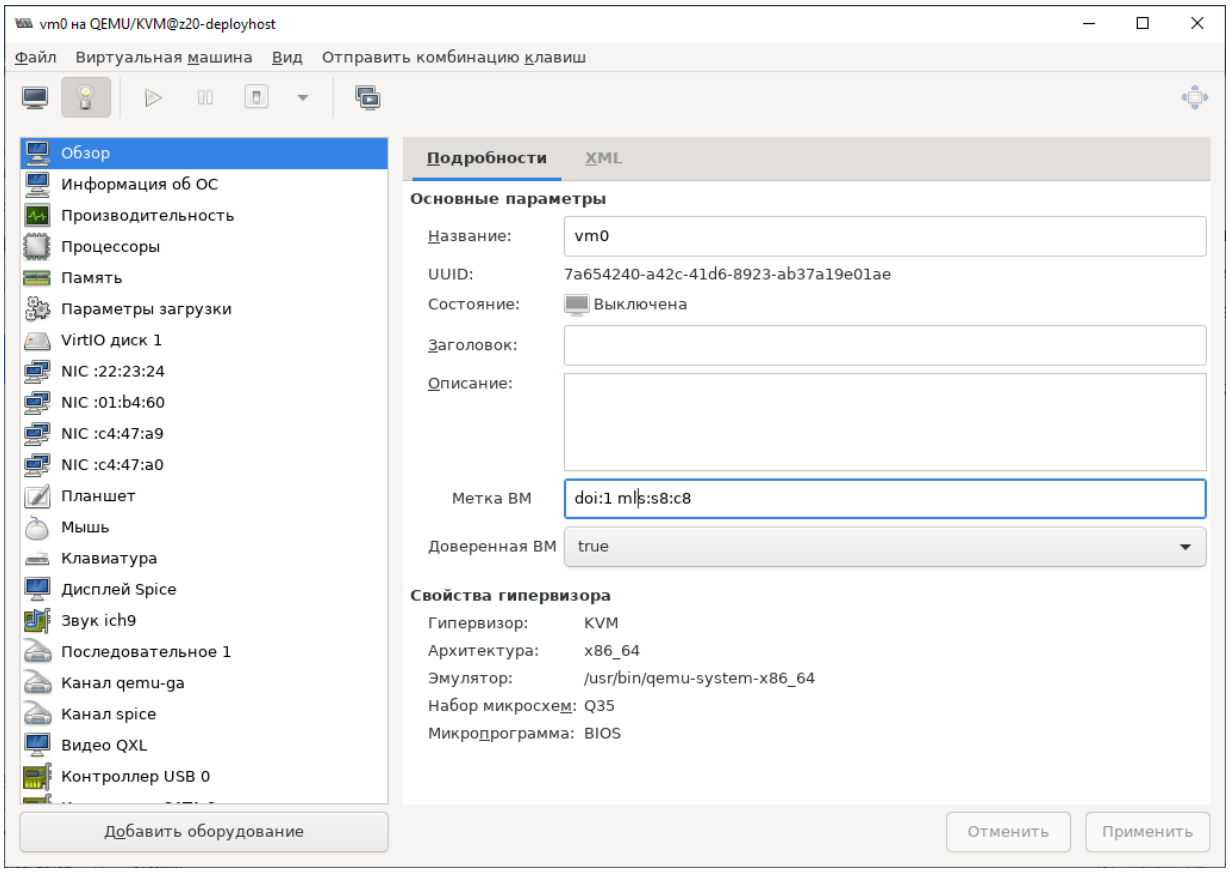

Рис. 31 – Метка виртуальной машины
в окне свойств виртуальной машины

Метки сетевых интерфейсов виртуальной машины. Метка или диапазон меток, который может быть использован виртуальными сетевыми интерфейсами в виртуальной машине должен входить в диапазон метки виртуальной машины. Для таких меток допустимо указывать дополнительные атрибуты, такие как: UNAWARE (для задания метки без требования к маркировке пакетов), порты TCP, UDP, SCTP для обеспечения многометочного обмена.

Например, чтобы создать виртуальный сетевой адрес с меткой «doi:1 mls:s8:c8 unaware» (рис. 32) необходимо выполнить следующие действия:

1. Выбрать элемент «Добавить оборудование» в окне свойств;

2. Выбрать элемент Сеть;

3. Указать имя устройства (сетевой мост, к которому будет подключено виртуальное сетевое устройство), имя виртуального устройства (имя виртуального устройства для сетевого интерфейса ВМ на стороне гипервизора), mac адрес устройства, ipv4 адрес, желаемую метку сетевого интерфейса.

Для обеспечения многометочного обмена (MLS меток) необходимо указать порты взаимодействия, а для однометочных адресов допустимо использовать атрибут UNAWARE без указания портов.

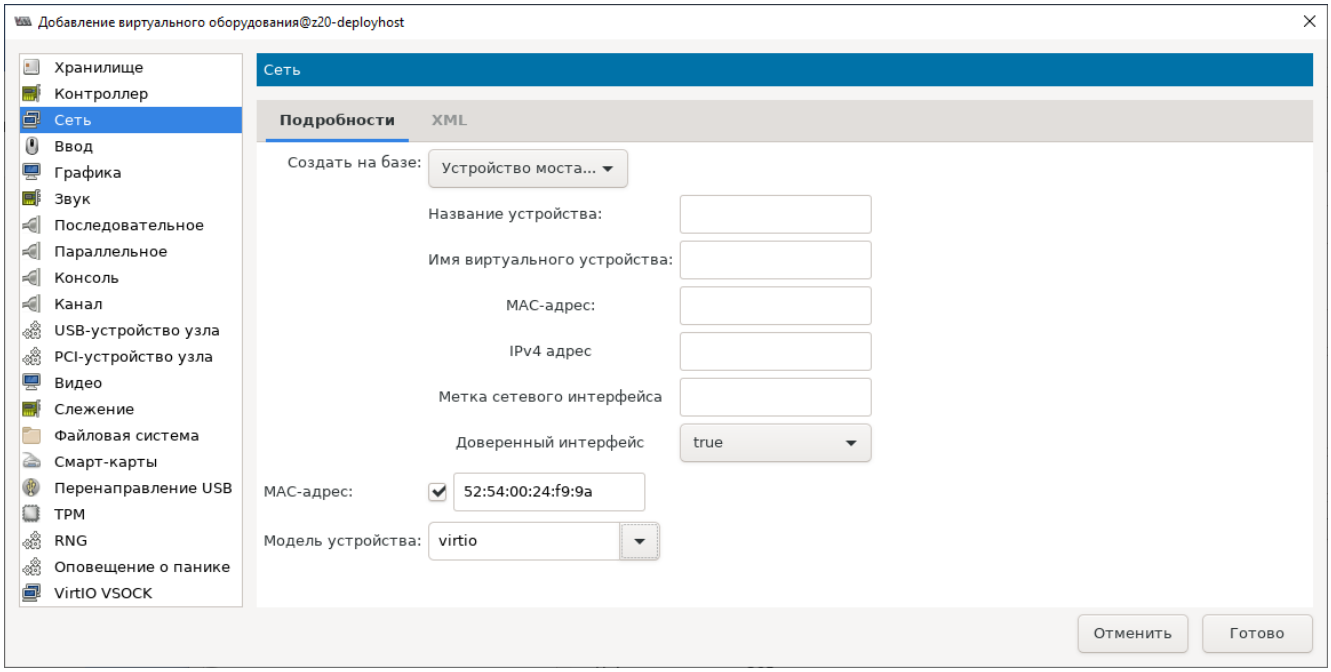

Рис. 32 – Назначение метки
сетевому интерфейсу

Развертывание виртуальных машин

Для создания виртуальной машины необходимо:

1. В главном окне необходимо нажать на меню «Файл» и выбрать пункт «Создать виртуальную машину» (рис. 33).

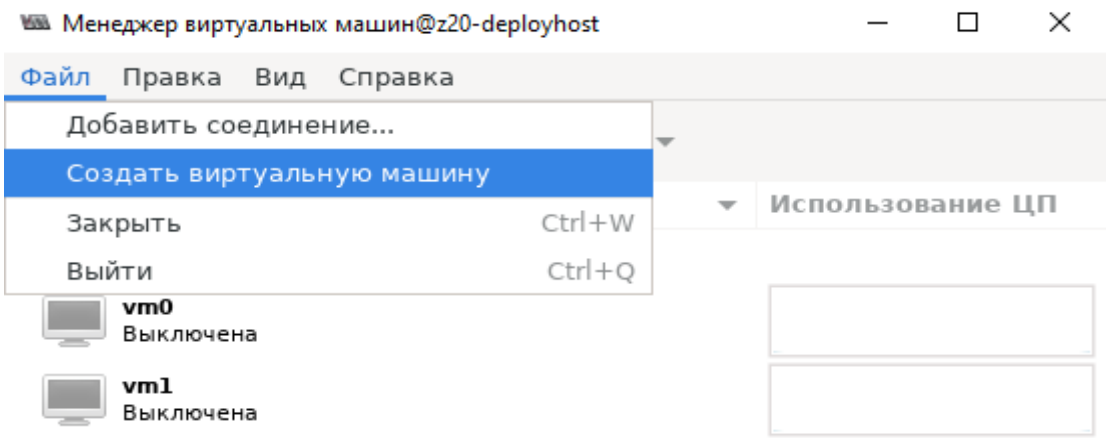

Рис. 33 – Создание виртуальной машины

В отобразившемся окне выбрать способ установки ОС виртуальной машины.

2. Настроить параметры ресурсов ВМ, для этого необходимо установить количество выделяемой памяти и количество процессоров (рис. 34).

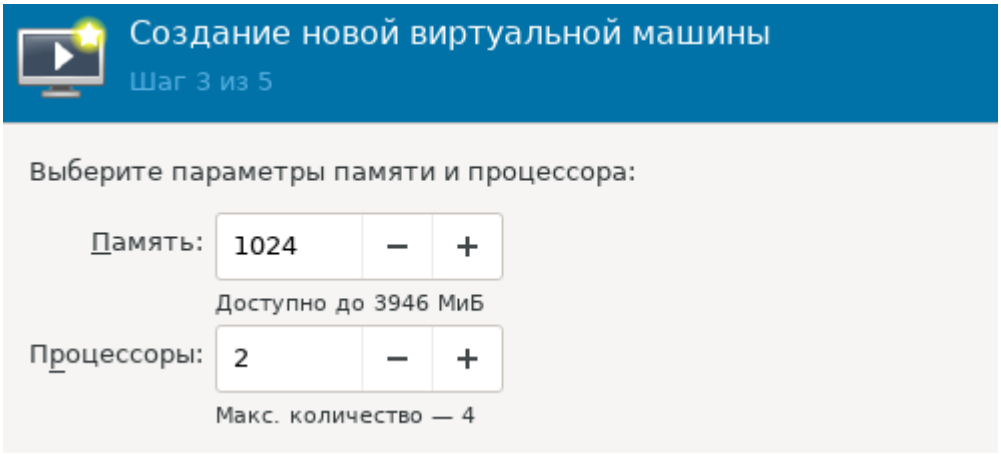

Рис. 34 – Настройка параметров ВМ

3. Настроить используемое хранилище для данных виртуальной машины (рис. 35).

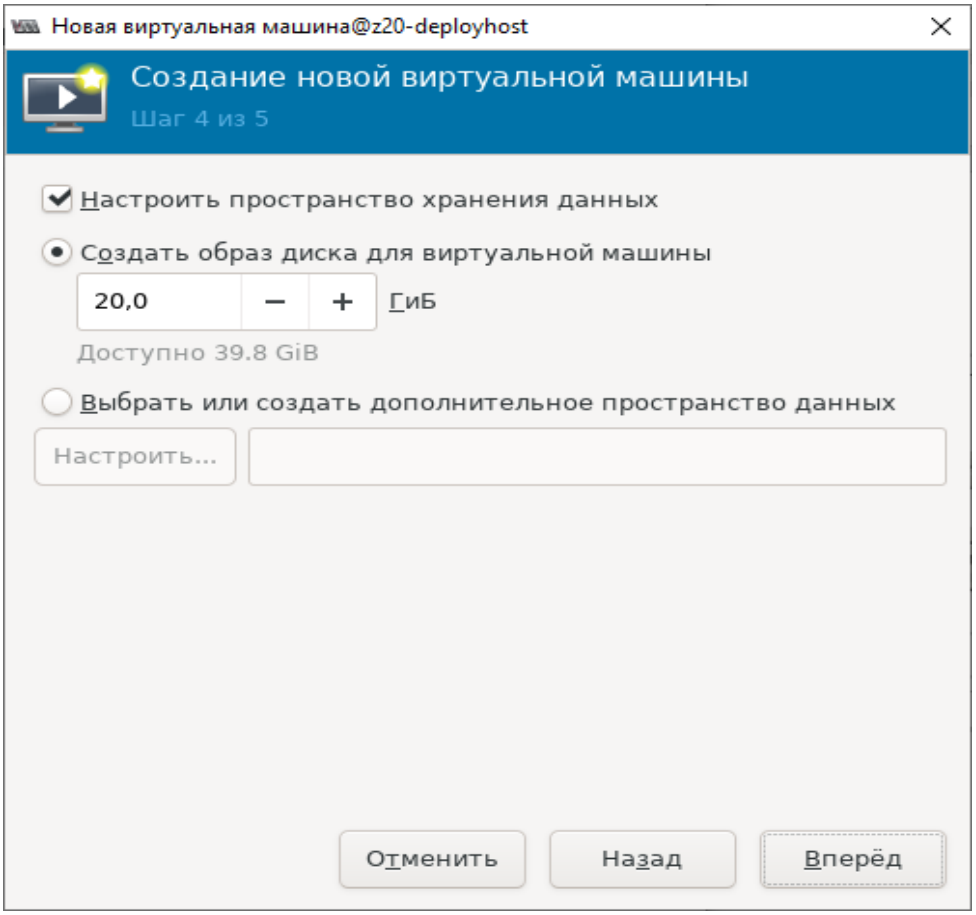

Рис. 35 – Настройка хранилища данных ВМ

4. Настроить метку виртуальной машины, признак доверенности, виртуальное сетевое устройство для виртуальной машины, указав необходимые реквизиты (рис. 36).

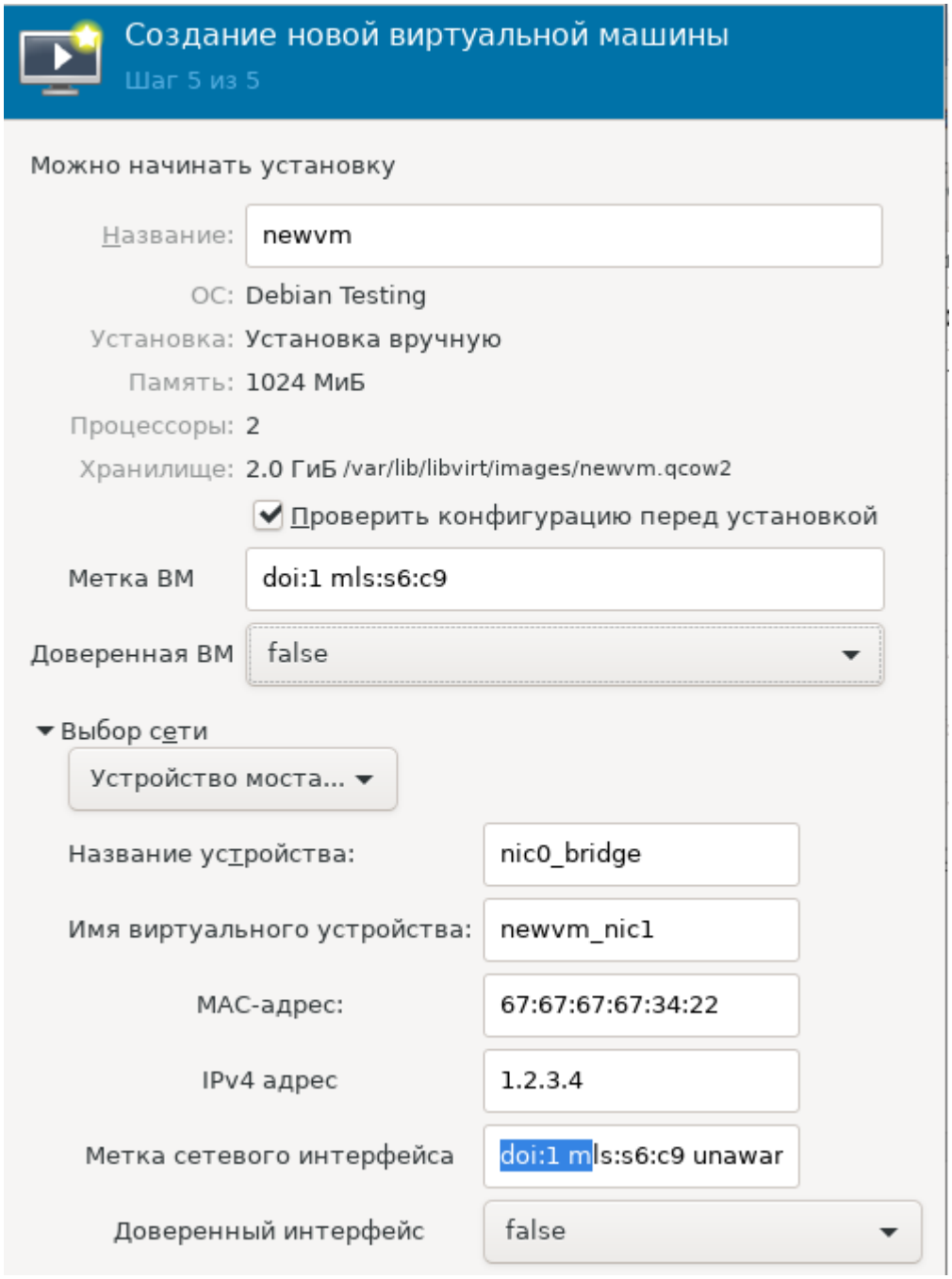

Рис. 36 – Окончательная настройка виртуальной машины

5. Можно указать флаг «Проверить конфигурацию перед установкой» для корректировки дополнительных параметров виртуальной машины (рис. 37).

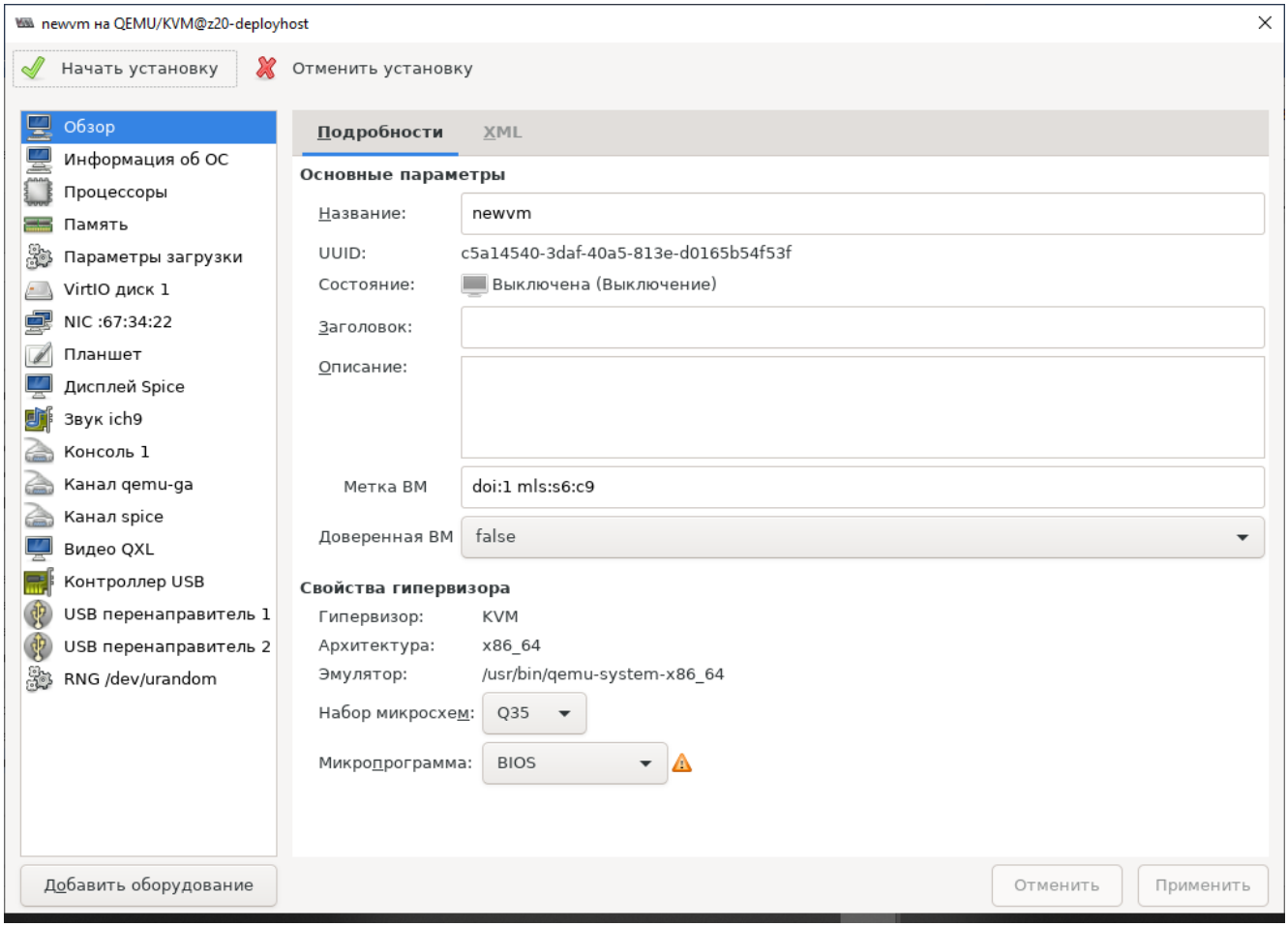

Рис. 37 – Дополнительные параметры виртуальной машины

3.5. Установка и настройка аппаратно-программного модуля доверенной загрузки

При эксплуатации ОС «Циркон 37С» самостоятельно на рабочей станции, в составе рабочей станции должен применяться аппаратно-программный модуль доверенной загрузки.

Внимание. *Ниже приведено краткое описание установки и настройки аппаратно-программного модуля доверенной загрузки. Полное и подробное описание установки и настройки аппаратно-программного модуля доверенной загрузки приведено в документации на используемый аппаратно-программный модуль доверенной загрузки*.

Для установки аппаратно-программного модуля доверенной загрузки необходимо выполнить следующие действия:

1. Установить программное обеспечение.
2. Установить плату.
3. Инициализировать изделие.
4. Подготовить изделие к эксплуатации.

Установка программного обеспечения производится согласно документации на используемый аппаратно-программный модуль доверенной загрузки.

Установка платы:

1. Выключить компьютер (рабочую станцию) если был включен, открыть корпус компьютера.
2. Установить переключатель SW1-1 платы в положение OFF.
3. Установить плату аппаратно-программного модуля доверенной загрузки в разъем системной шины PCI-E.

Инициализация аппаратно-программного модуля доверенной загрузки:

1. Включить питание компьютера. Управление передается аппаратно-программному модулю доверенной загрузки.

2. На экране появится диалоговое окно, в котором необходимо выбрать пункт «Инициализация платы» и нажать клавишу ввода.

3. Настройка общих параметров. На экране появится диалоговое окно с общими параметрами системы. Выполнить необходимую настройку.

4. Зарегистрировать администратора.

Подготовка к эксплуатации

Для подготовки к эксплуатации:

1. Выключить компьютер, открыть корпус компьютера.

2. Извлечь плату из разъема шины PCI-E.

3. Установить переключатель SW1-1 в положение ON.

4. Установить плату в разъем системной шины PCI-E.

5. Подключить к плате считыватель электронного идентификатора «таблетки».

6. Закрыть корпус компьютера.

Настройка и эксплуатация изделия

1. Включить питание компьютера или выполнить перезагрузку компьютера.

На экране появится окно с запросом персонального идентификатора.

2. Предъявить персональный идентификатор администратора.

3. Ввести пароль администратора.

4. На экране появится меню администратора.

5. Выбрать пункт «Список пользователей». На экране появится диалоговое окно.

6. Создать нового пользователя и зарегистрировать новый идентификатор «таблетки» для него.

4. Руководство пользователя

4.1. Начало и завершение работы на терминальном устройстве

4.1.1. Работа с сессией

Вход в сессию

Предварительные требования:

- к терминальному устройству должны быть подключены монитор, клавиатура с кардридером и «мышь».

Для входа в сессию необходимо:

1. Вставить карту в кардридер.

2. Дождаться пока терминальное устройство считает данные с карты.

3. В появившемся окне ввести в поле «Пароль» личный пароль пользователя (рис. 38).

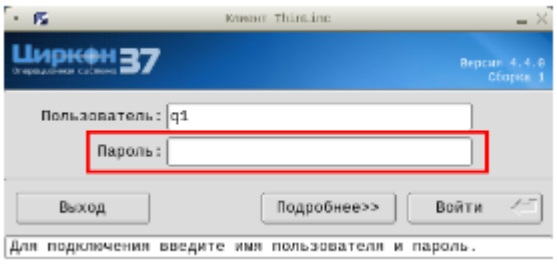

Рис. 38 – Поле ввода пароля

Выход из сессии

Для выхода из сессии необходимо:

1. Завершить сессию стандартным способом:

- Нажать на кнопку главного Меню (рис. 39).
- Выбрать пункт «Завершить сеанс пользователя...» (рис. 39).

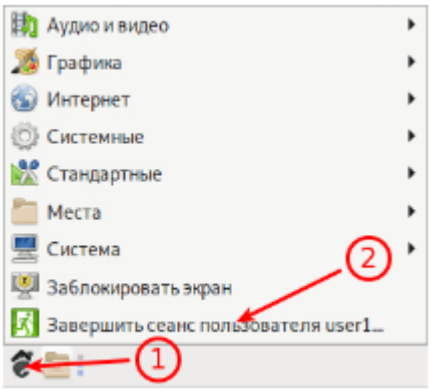

Рис. 39 – Завершение сессии

- Нажать «Завершить сеанс» (рис. 40).

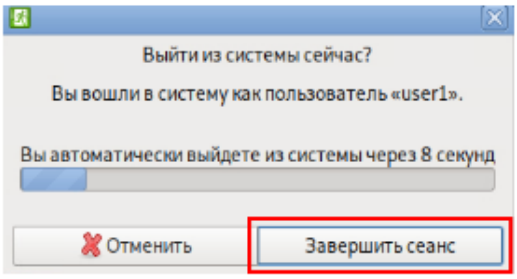

Рис. 40 – Завершение сессии

2. Вынуть карту из кардридера.

Примечание. *Допускается вынимать карту из кардридера без завершения сессии. В таком случае сессия будет заблокирована. Вход в заблокированную сессию осуществляется стандартным способом*.

Подключение к заблокированной сессии

Параметр «Завершить сеанс» (рис. 41) позволяет при подключении к заблокированной сессии сперва завершить ее, а затем создать новую.

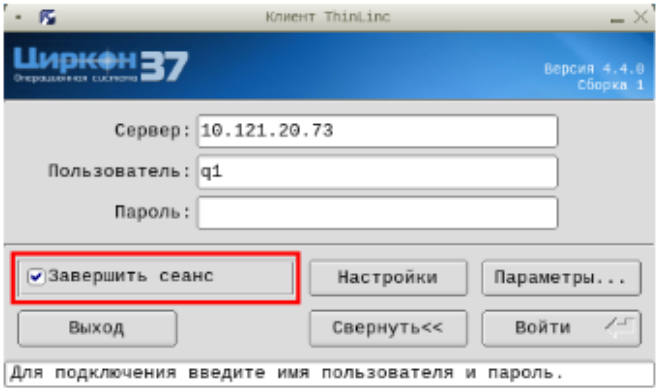

Рис. 41 – Завершение сеанса

4.2. Начало и завершение работы на рабочей станции

1. Для загрузки системы необходимо включить рабочую станцию. Загрузка производится в автоматическом режиме и не требует участия пользователя.

2. После запуска рабочей станции управление передается установленному аппаратно-программному модулю доверенной загрузки. На экране появится диалоговое окно с запросом персонального идентификатора.

3. Предъявить выданный пользователю персональный идентификатор (для электронного идентификатора «таблетки» – плотно приложить идентификатор к считывателю).

4. После успешного считывания информации из идентификатора на экране появится диалоговое окно для ввода пароля.

5. Ввести пароль.

6. Если предъявлен незарегистрированный идентификатор или введен неверный пароль, в строке сообщений появится сообщение «Неверный идентификатор или пароль». Нажать любую клавишу и повторить еще раз действия приведенные выше.

7. После успешного выполнения всех действий на экране появится меню пользователя. Выбрать пункт «Загрузка операционной системы». При этом начнется штатная загрузка ОС «Циркон 37С».

8. После загрузки ОС «Циркон 37С» на экран будет выведено приглашение на вход под учетной записью пользователя. Необходимо ввести в поле пароль, выданный администратором, и нажать на кнопку «Войти», либо клавишу <Enter>.

9. ОС «Циркон 37С» готова к работе.

Для завершения работы необходимо:

- Нажать на кнопку главного Меню (см. рис. 39).
- Выбрать пункт «Завершить сеанс пользователя...» (см. рис. 39).
- Нажать «Завершить сеанс» (см. рис. 40).

4.3. Графический вход в программу

После входа в учетную запись пользователя на экран выводится рабочий стол. На рис. 42 показан вид рабочего стола после загрузки программы.

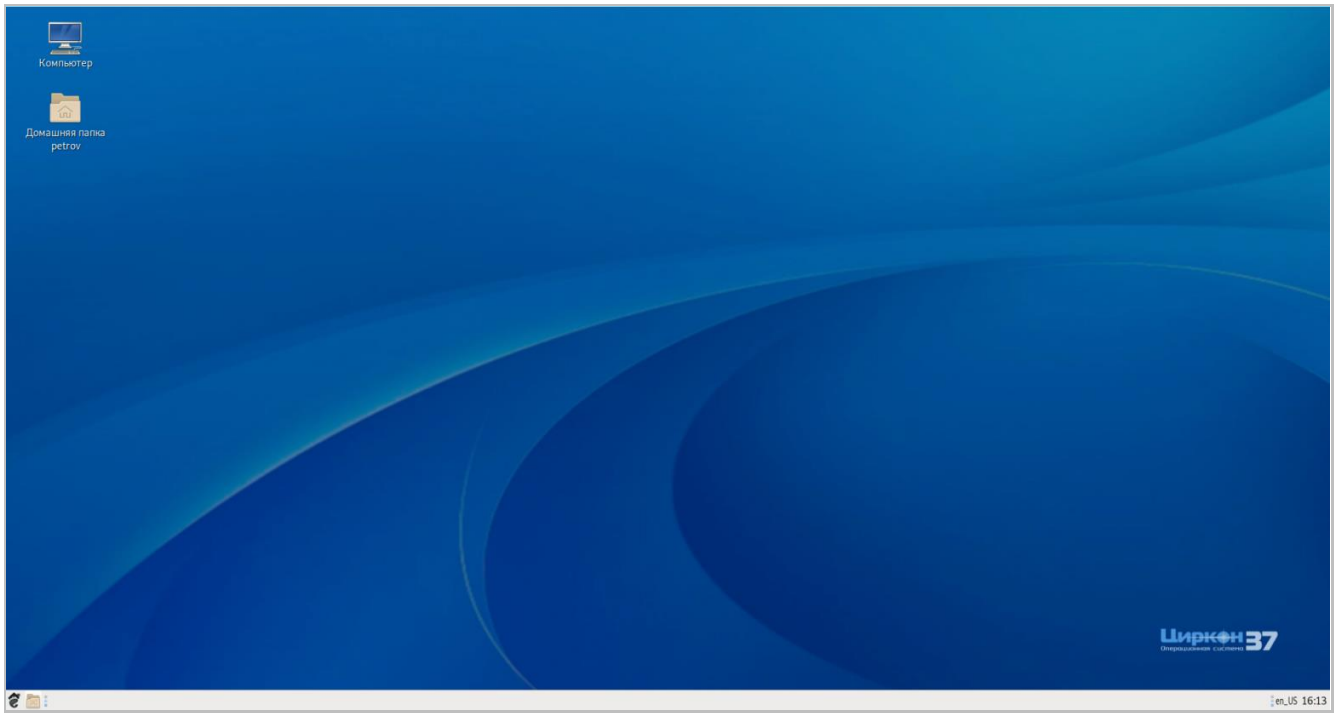

Рис. 42 – Рабочий стол

Для работы с графическим интерфейсом программы используются клавиатура и «мышь».

4.4. Блокировка экрана

Блокировка экрана предотвращает несанкционированный доступ к приложениям и информации пользователя. На время блокировки экрана будет включен скринсейвер.

Чтобы заблокировать экран, выбрать из главного Меню «Заблокировать экран» (рис. 43).

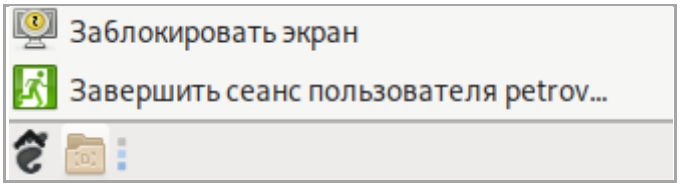

Рис. 43 – Блокировка экрана

Чтобы разблокировать экран, подвигать «мышь» или нажать любую клавишу, ввести свой пароль в диалоговом окне заблокированного экрана (рис. 44), затем нажать клавишу «Enter» .

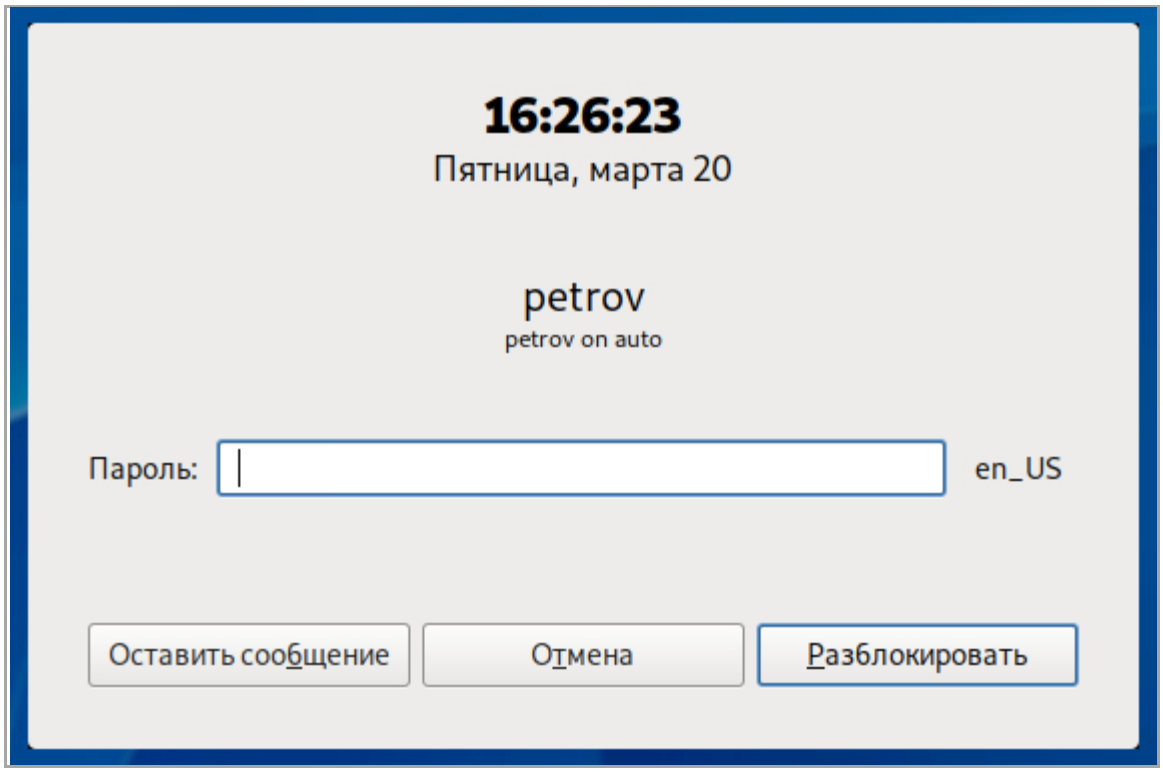

Рис. 44 – Диалоговое окно заблокированного экрана

Можно оставить сообщение пользователю, который заблокировал свой экран. Для этого следует подвигать «мышь» или нажать клавишу на клавиатуре и нажать на кнопку «Оставить сообщение». Ввести сообщение в поле ввода и нажать кнопку «Сохранить» (рис. 45).

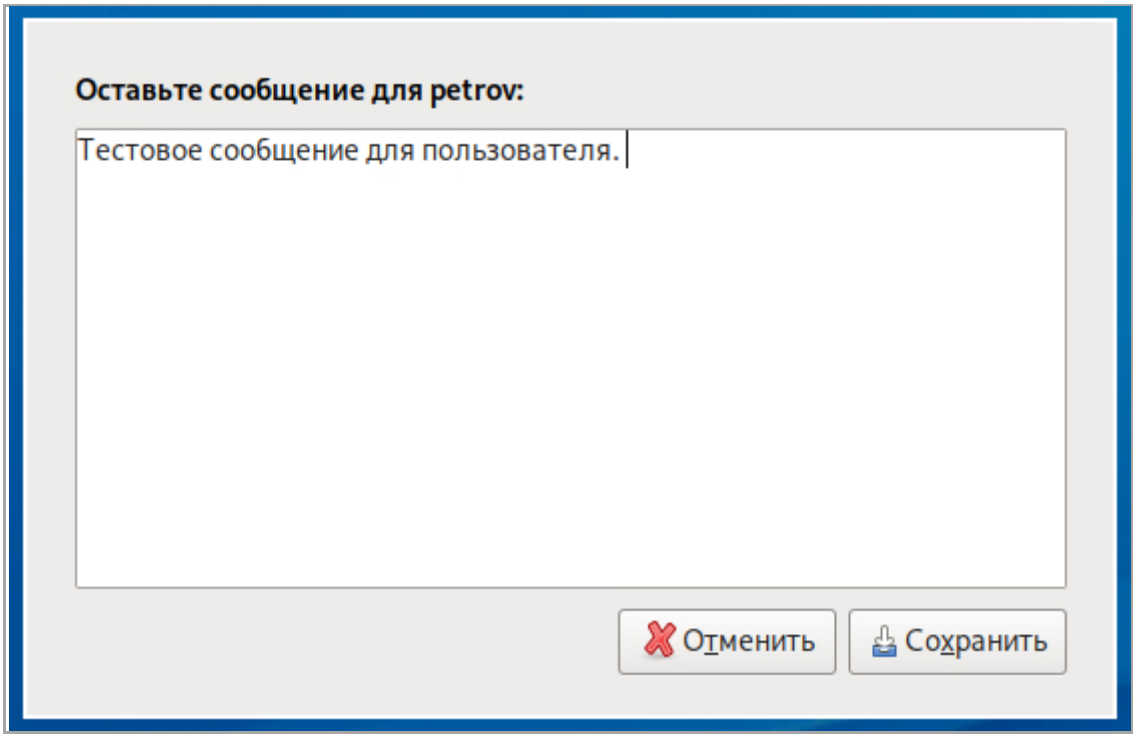

Рис. 45 – Поле ввода сообщений

Сообщение будет отображено в верхнем правом углу рабочего стола, когда пользователь разблокирует экран.

4.5. Настройка автоматического запуска программ

Можно выбрать определенные программы, которые будет запущены автоматически при входе в сеанс. Например, можно настроить так, чтобы браузер запускался сразу после входа в систему. Программы, которые запустятся автоматически при входе в систему, называются автозапускаемые программы. Автозапускаемые программы автоматически сохраняют свое состояние и безопасно завершаются сеансовым менеджером при выходе из системы и перезапускаются при входе.

Для настройки автоматического запуска программ зайти в «Меню» - «Система» - «Параметры» - «Персональные» - «Запускаемые приложения».

Инструмент настройки сессии «Запускаемые приложения» позволяет настроить, какие программы будут автоматически запущены при входе в систему. У него есть две вкладки – «Автоматически запускаемые программы» и «Опции» (рис. 46).

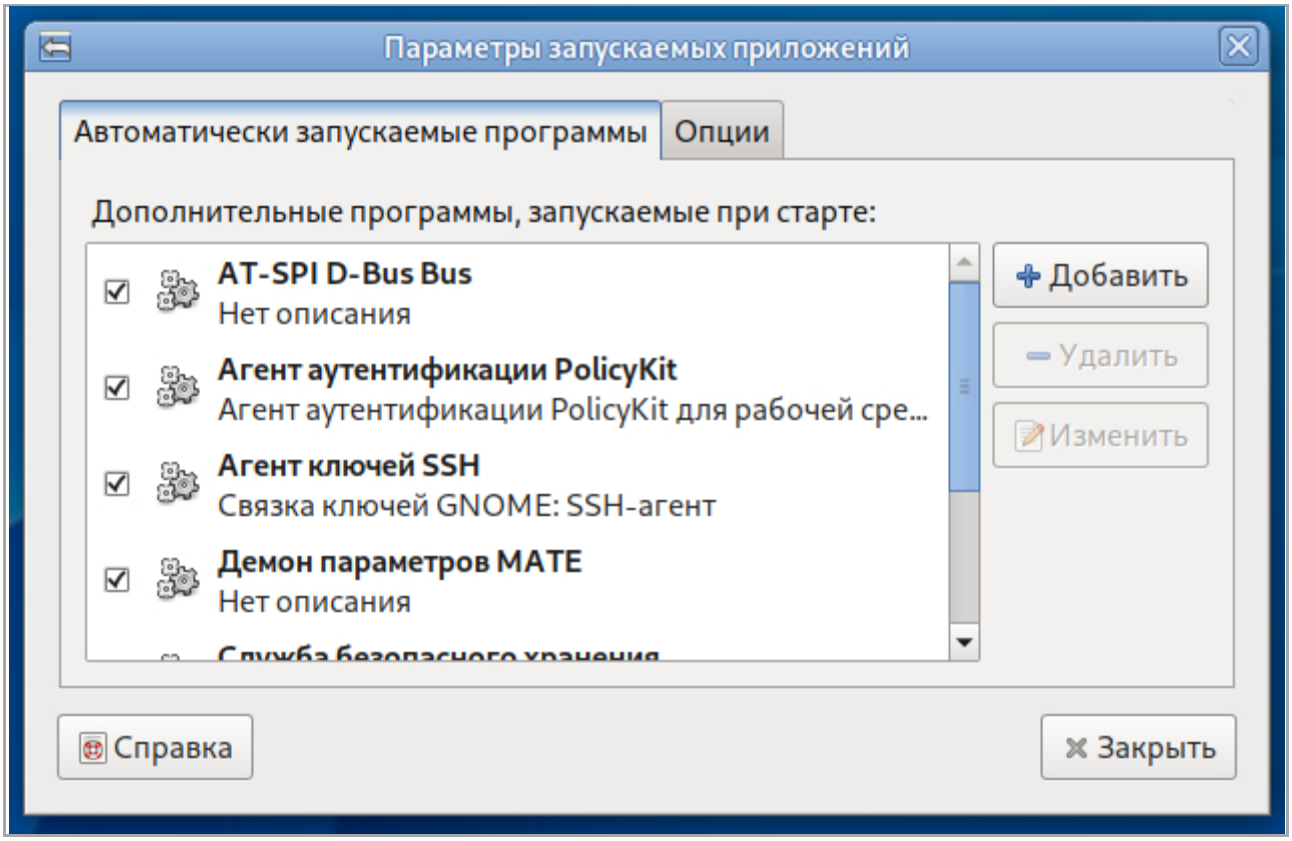

Рис. 46 – Вкладка «Автоматически запускаемые программы»

При выборе вкладки «Автоматически запускаемые программы» появляется список автоматически запускаемых программ. Этот список содержит краткое описание каждой программы и галочку, указывающую запускать программу или нет. Программы, не выбранные для запуска, не будут запущены автоматически при входе в систему. Во вкладке «Автоматически запускаемые программы» можно добавить, удалить и изменить автозапускаемые приложения.

Для включения автоматического запуска программы необходимо установить галочку (рис. 47).

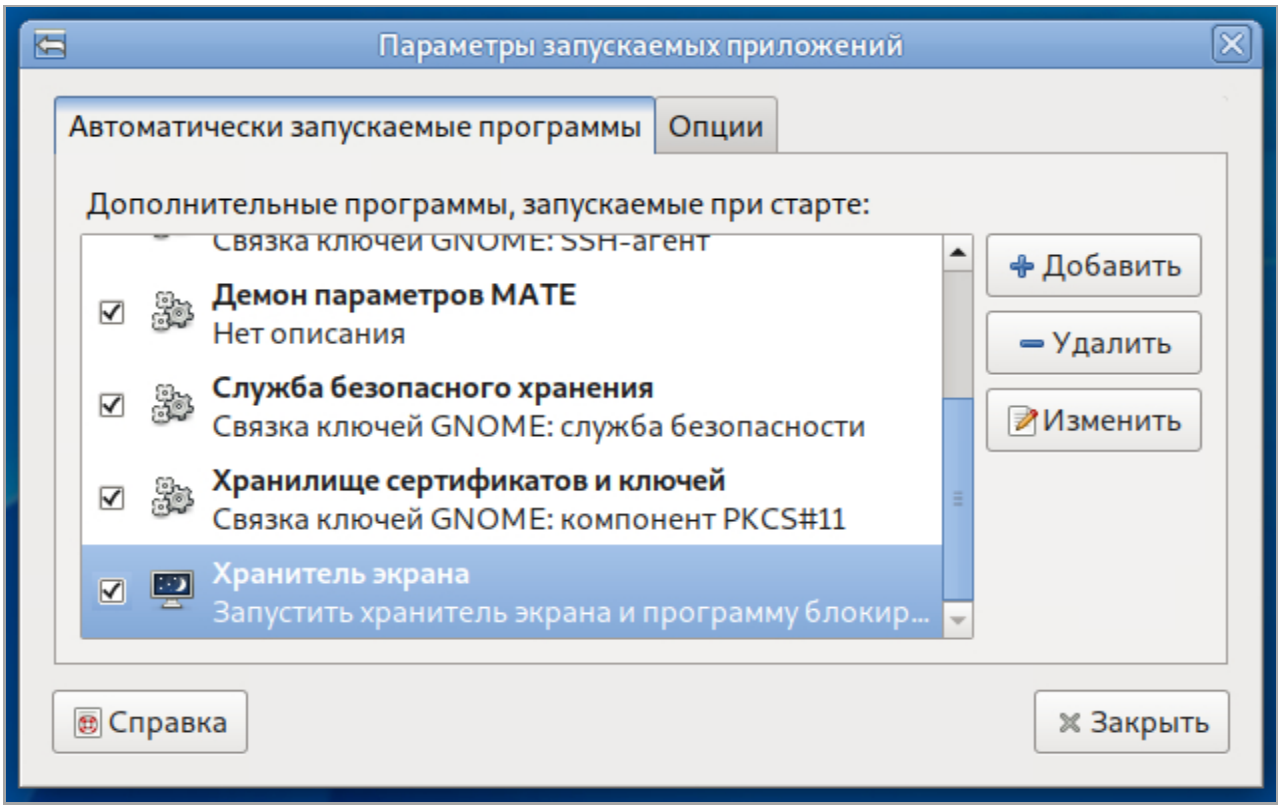

Рис. 47 – Вкладка «Автоматически запускаемые программы». Установка галочки

Для отключения автоматического запуска программы необходимо снять галочку (рис. 48).

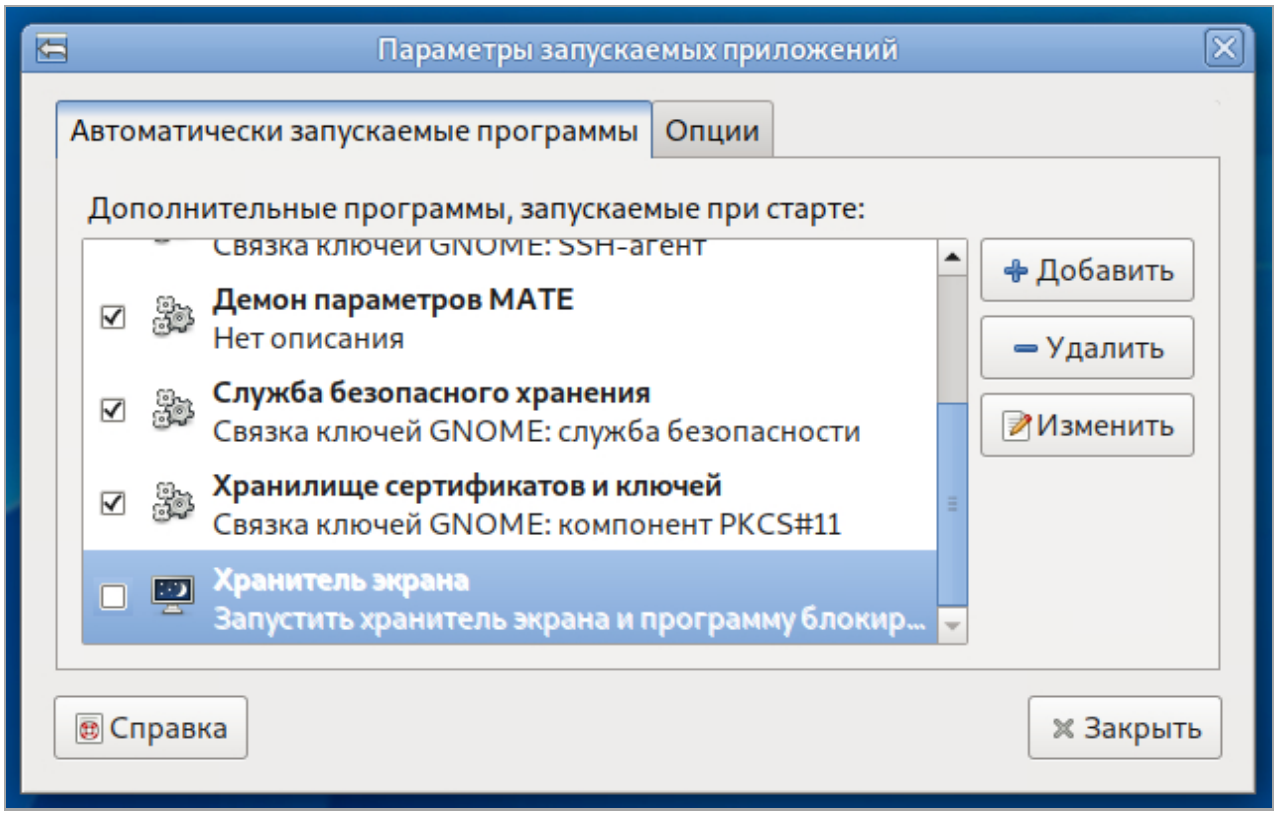

Рис. 48 – Вкладка «Автоматически запускаемые программы». Снятие галочки

Добавление новых программ для автозапуска

Чтобы добавить новую программу для запуска, необходимо выполнить следующие действия:

1. Нажать кнопку «Добавить». Откроется окно «Новая автоматически запускаемая программа» (рис. 49).

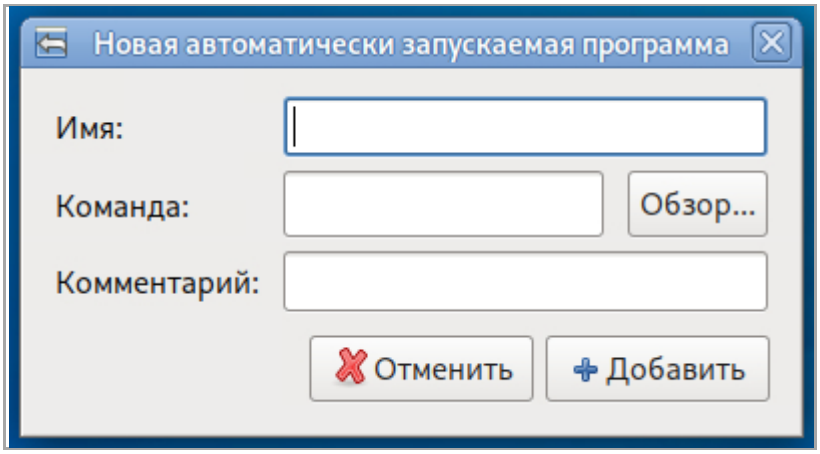

Рис. 49 – Окно «Новая автоматически запускаемая программа»

2. В поле ввода «Имя» ввести имя новой программы запускаемой автоматически.

3. В поле ввода «Команда» указать команду, которая запустит приложение. Например, команда «pluma» запустит текстовый редактор Pluma. Если команда не известна, следует нажать «Обзор» для выбора пути команды.

4. Ввести описание приложения в поле «Комментарии». Это описание программы будет видно в списке автозапускаемых программ.

5. Нажать кнопку «Добавить». Приложение будет добавлено в список автозапускаемых программ, с проставленной галочкой напротив него.

Удаление из настроек автозапускаемой программы

Для удаления автозапускаемой программы необходимо выбрать ее из списка и нажать кнопку «Удалить».

Редактирование программы запускаемой автоматически

Для редактирования существующей автозапускаемой программы необходимо выбрать ее из списка автозапускаемых программ и нажать кнопку «Изменить».

Менеджер сеанса может запомнить какие приложения были запущены при выходе из системы и автоматически запустить их при входе в систему. Если необходимо, чтобы это происходило каждый раз при выходе из системы, включить «Автоматически запоминать запущенные приложения при выходе из сеанса» во вкладке «Опции» окна «Параметры запускаемых приложений» (рис. 50).

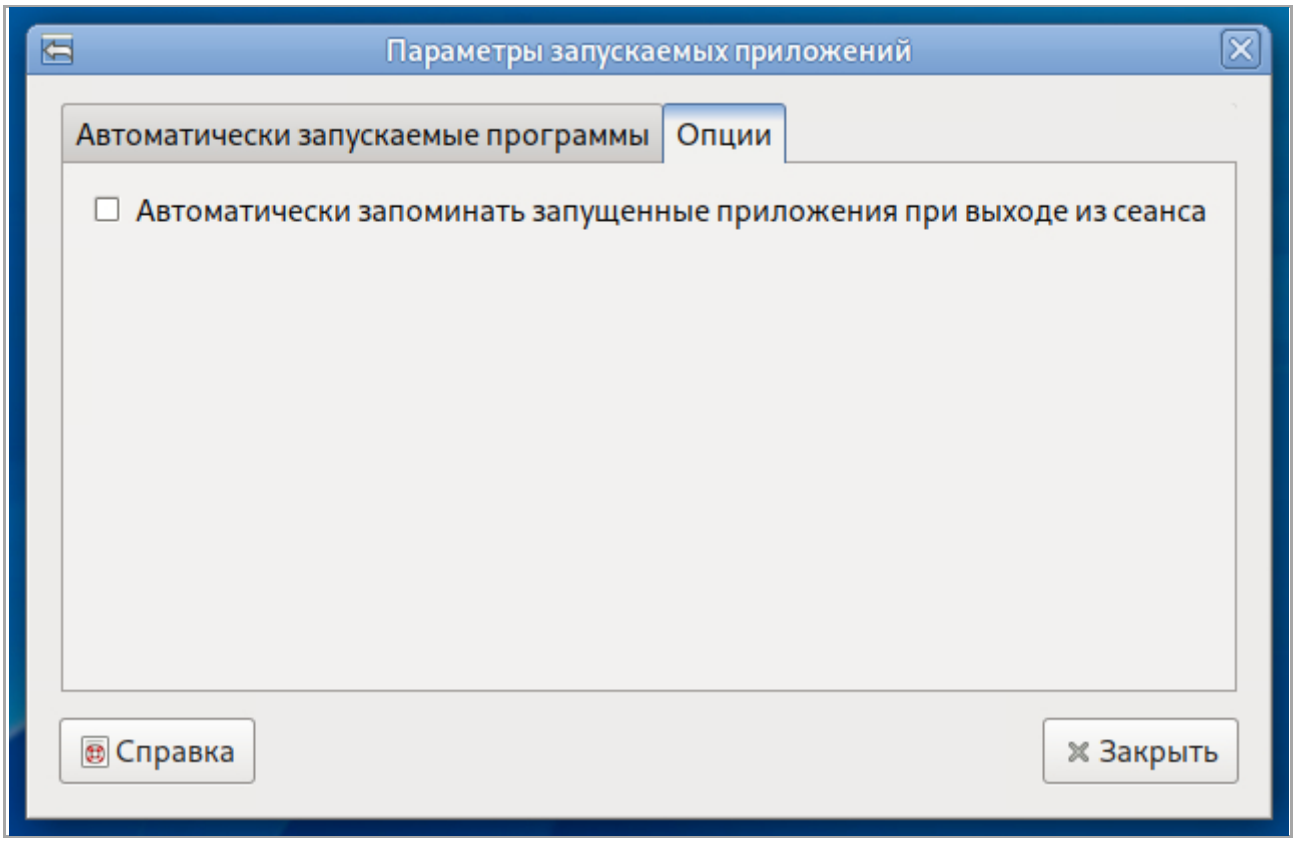

Рис. 50 – Вкладка «Опции»

5. Рабочий стол MATE

Рабочий стол MATE предоставляет пользователю:

1. Графический вход в программу.

2. Рабочий стол для размещения элементов графического интерфейса.

3. Значки на рабочем столе, представляющие как файлы и/или каталоги, так и ярлыки для программ, приложений, устройств, ссылок.

4. Панель рабочего стола.

5. Меню приложений, доступное через кнопку главного Меню.

6. Высокую гибкость в настройке, как внешнего вида, так и процесса функционирования рабочего стола, значков и окон приложений, панелей и их реквизитов. Практически каждый элемент рабочего стола имеет контекстное меню, вызываемое нажатием правой кнопки «мыши», позволяющее выполнять его настройку с помощью этого меню.

7. Набор приложений для повседневного использования (файловый менеджер, текстовый редактор и т.п.).

8. Различные диалоги для ситуаций, когда требуется реакция пользователя, например диалог завершения работы.

5.1. Рабочий стол

Рабочим столом (см. рис. 42) называется экран, отображаемый после загрузки. Рабочий стол состоит из пространства (поля) рабочего стола и находящейся в нижней части главной панели рабочего стола. Практически каждый элемент пользовательского интерфейса рабочего стола имеет контекстное меню, позволяющее выполнять его настройку непосредственно с помощью этого меню.

После установки в поле рабочего стола обычно располагаются ярлык «Компьютер» и домашняя папка пользователя.

При подключении флеш-диска, других съемных носителей или устройства, содержащего файлы (например, аудиоплеер или цифровая камера) на рабочем столе появляется значок подключенного устройства.

Файловый менеджер Caja обеспечивает доступ к файлам, папкам и приложениям. Через него можно управлять содержимым папок и открывать файлы в соответствующих приложениях.

На рабочем столе можно размещать значки наиболее часто используемых программ, документов, устройств. Приложение открывается после двойного нажатия левой кнопкой «мыши» на значок приложения.

После нажатия правой кнопкой «мыши» на значок приложения появляется контекстное меню, которое позволяет открыть приложение и выполнить определенные операции:

- «Открыть»;
- «Открыть в другой программе»;
- «Вырезать»;
- «Копировать»;
- «Создать ссылку»;
- «Переименовать…»;
- «Копировать в»;
- «Переместить в»;
- «Удалить в корзину»;
- «Удалить»;
- «Изменить размер значка…»;
- «Вернуть исходный размер значка»;
- «Свойства».

Можно настроить компьютер, используя «Центр управления», расположенный в меню «Система». Каждый из инструментов настройки в центре управления позволяет изменять определенные настройки компьютера.

Панель рабочего стола

Панель рабочего стола содержит:

1. Кнопку главного Меню;
2. Апплеты:
   - Кнопка расчистки рабочего стола;
   - Список окон;
   - Область уведомления;
   - Часы;
   - Индикатор раскладки клавиатуры, параметры клавиатуры, текущая раскладка.

Кнопка главного Меню

Кнопка главного Меню  расположена слева на главной панели. Нажатием левой кнопки «мыши» на кнопку главного меню раскрывается меню, с помощью которого можно быстро запускать приложения. Стартовое меню представлено на рис. 51.

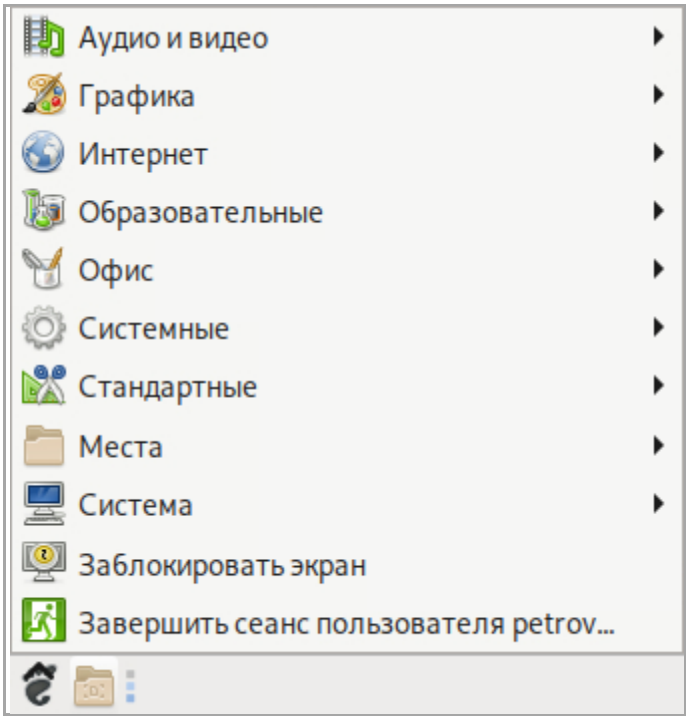

Рис. 51 – Стартовое меню

Апплеты

Меню апплетов вызывается нажатием правой кнопки «мыши».

Кнопка расчистки рабочего стола  сворачивает все окна.

Список окон. Отображает вкладку каждого открытого окна. Список окон позволяет сворачивать и разворачивать окно, при нажатии на вкладку с названием окна.

Меню индикатора раскладки клавиатуры позволяет переключить раскладку клавиатуры, посмотреть параметры клавиатуры и текущую раскладку.

Апплет Часы отображает текущие время и дату. После наведения курсора на часы появляется информация о текущем числе, месяце и дне недели.

5.2. Окна

Все приложения ОС «Циркон 37С», обладающие графическим интерфейсом, запускаются в окнах (рис. 52).

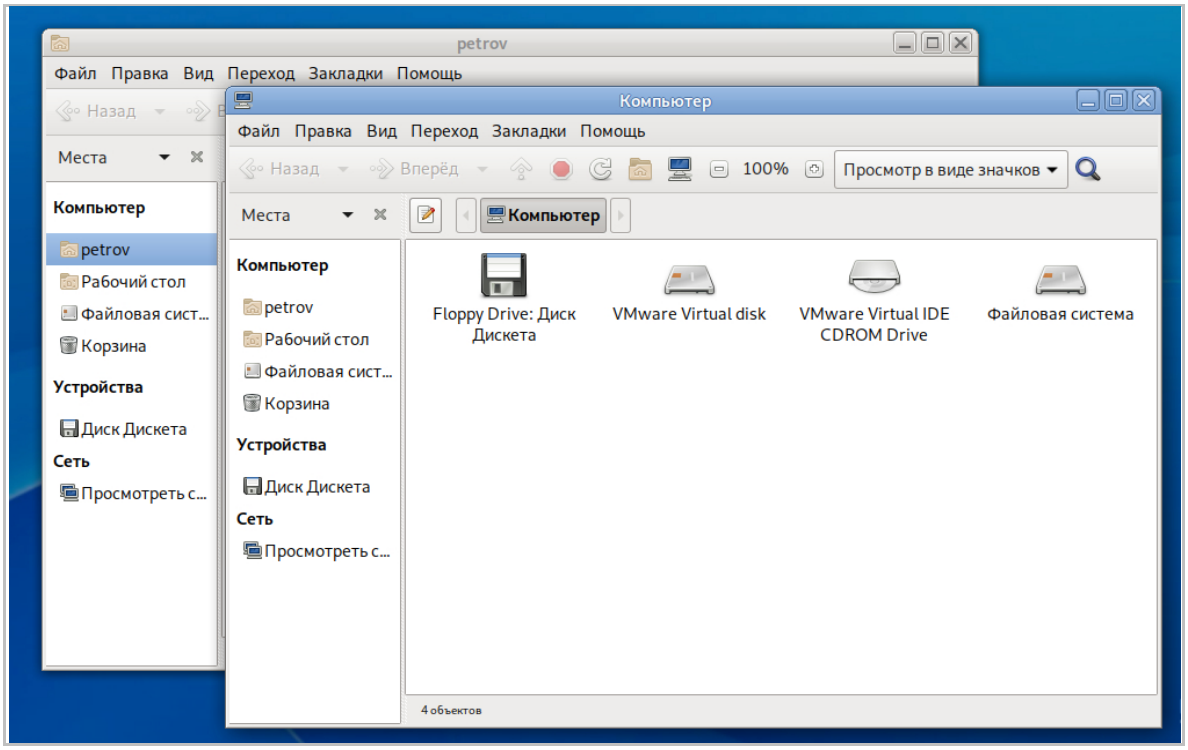

Рис. 52 – Окна

Окно приложения открывается после запуска программы, а закрытие окна приводит к завершению работы приложения.

Окно представляет собой ограниченную рамкой область экрана, внутри которой расположены функциональные элементы приложения. У окна имеется заголовок. В левой части заголовка находится пиктограмма приложения, в центральной – название окна, а в правой – кнопки управления окном.

Окна можно располагать на любом участке экрана. Чтобы переместить окно, необходимо перетащить его заголовок «мышью» в нужном направлении. Чтобы изменить размеры окна, нужно подвести курсор «мыши» к краям его рамки и перетащить их «мышью».

Одновременно может быть открыто несколько окон, при этом активное (используемое в текущий момент) окно отображается поверх остальных.

Чтобы сделать окно активным, необходимо щелкнуть внутри него «мышью».

Если содержимое окна целиком не помещается на экране, у правой границы окна появляется полоса прокрутки. В различных приложениях полосы прокрутки могут внешне отличаться друг от друга.

Диалоговые окна появляются по требованию окна приложения. Диалоговое окно может сообщать о проблеме, запрашивать подтверждение действия или ввод данных (рис. 53).

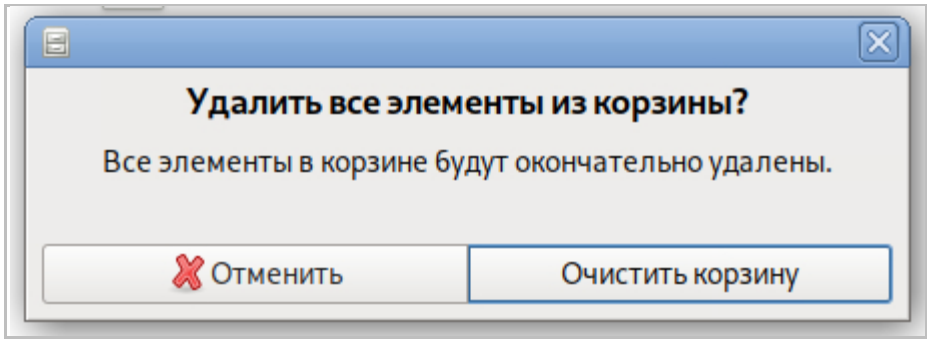

Рис. 53 – Диалоговое окно

5.3. Приложения

Приложение – это разновидность компьютерной программы, которая позволяет выполнять определенную задачу. Например, приложения используются для создания текстовых документов, работы с электронными таблицами, прослушивания музыки, работы в сети, для создания, правки и просмотра изображений и видеозаписей. Для каждой из этих задач нужно использовать отдельное приложение.

Ниже приведены некоторые приложения, входящих в состав графической среды MATE:

1. Текстовый редактор Pluma (рис. 54) позволяет просматривать, создавать или изменять любой простой (неформатированный) текст.

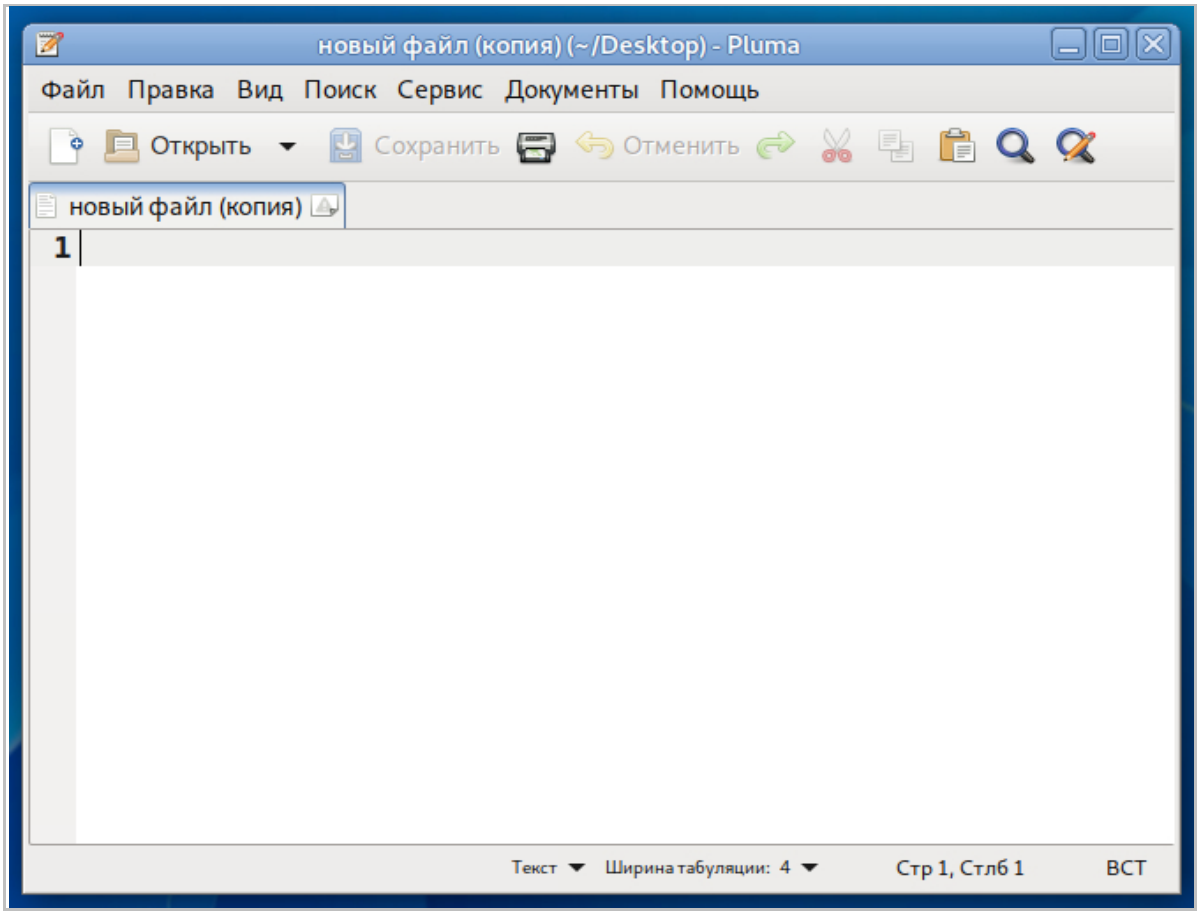

Рис. 54 – Текстовый редактор Pluma

2. Файловый менеджер Caja отображает папки и их содержимое (рис. 55). Используется для копирования, перемещения и сортировки файлов и для доступа к содержимому носителя данных, USB-флеш дисков или другим съемным носителям.

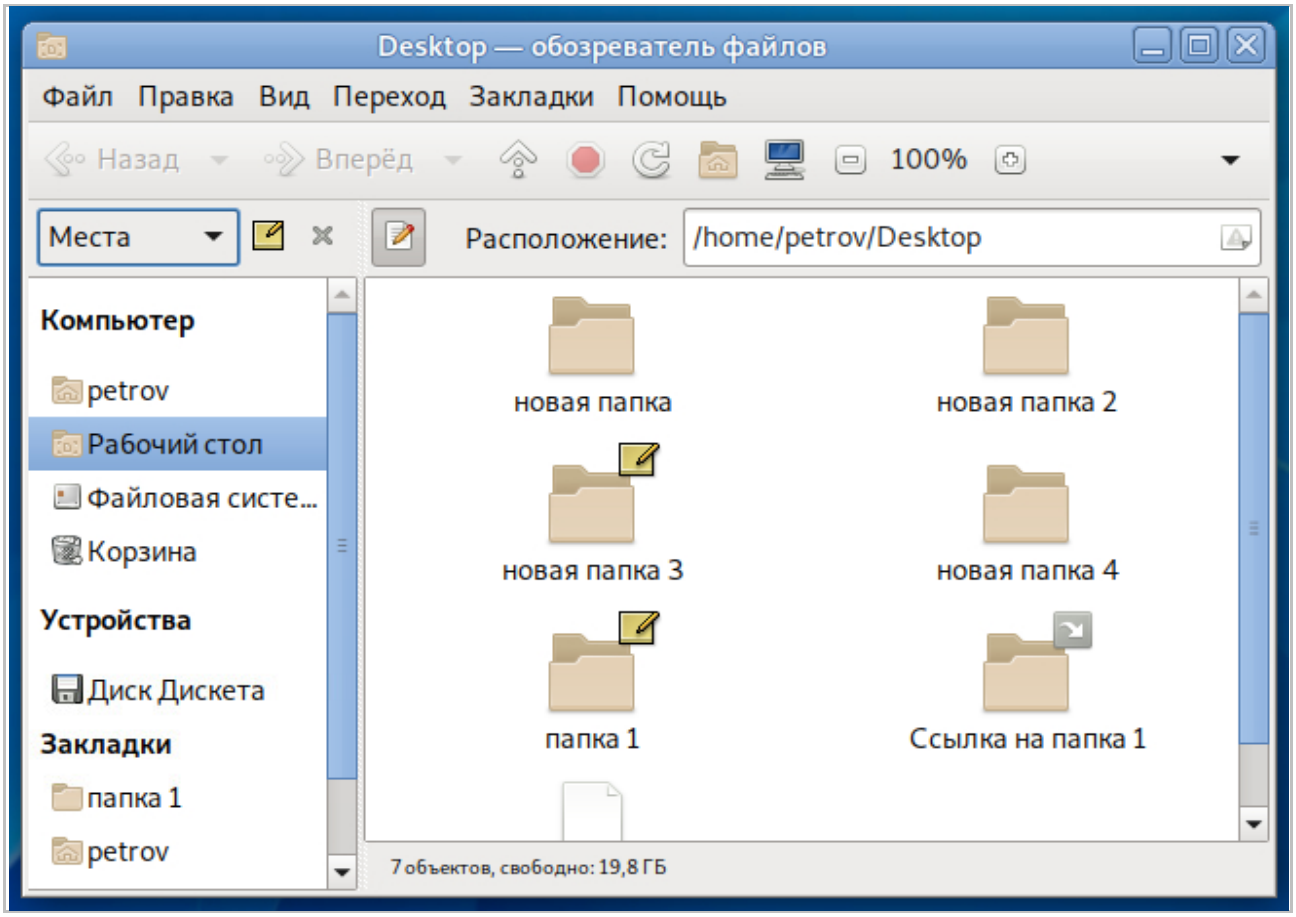

Рис. 55 – Файловый менеджер Caja

3. Терминал MATE обеспечивает доступ к системной командной строке (рис. 56).

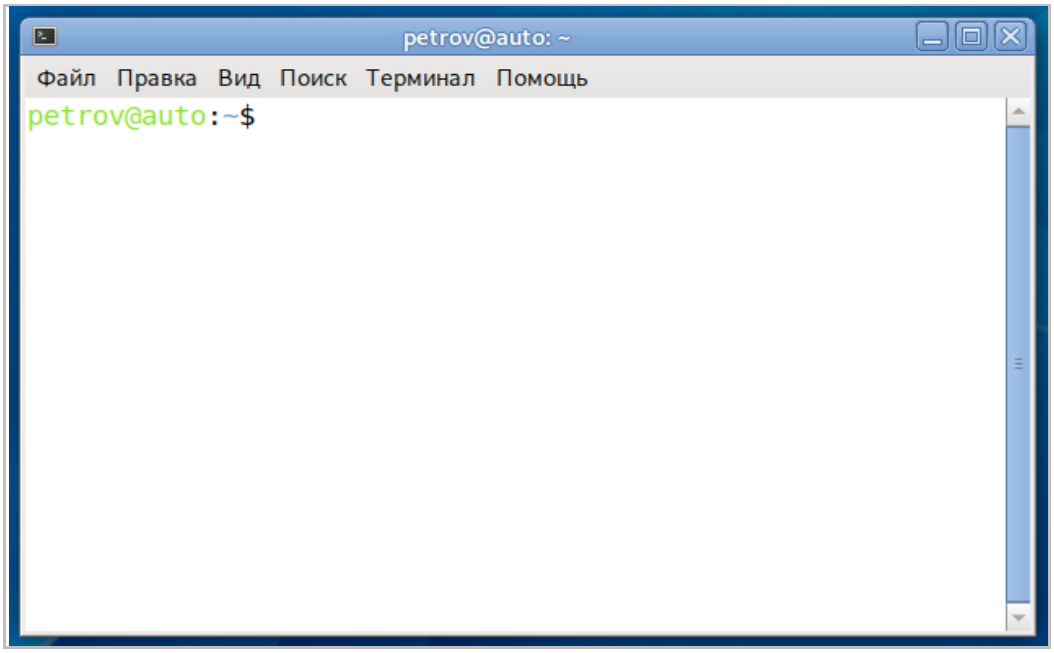

Рис. 56 – Терминал MATE

Стандартный набор приложений MATE включает в себя игры, музыкальные и видеоплееры, веб-браузер, приложения для обеспечения специальных возможностей, утилиты для настройки системы. Можно добавлять другие приложения, такие как текстовые и графические редакторы.

АКЦИОНЕРНОЕ ОБЩЕСТВО
"МНОГОПРОФИЛЬНОЕ
ВНЕДРЕНЧЕСКОЕ ПРЕДПРИЯТИЕ
"СВЕМЕЛ"

127254, г. Москва, Огородный пр., д. 5, стр.5
Тел/Факс: +7(495) 926-7187, +7(499) 750-7065
E-mail: post@swemel.ru