Для служебного пользования
Экз № ____

Утвержден

МБРЦ.468313.002-ЛУ

ПРОГРАММНОЕ ИЗДЕЛИЕ “БАЗОВЫЕ СРЕДСТВА ВИРТУАЛИЗАЦИИ ВЫЧИСЛИТЕЛЬНЫХ ПРОЦЕССОВ ЗАЩИЩЕННЫХ ОПЕРАЦИОННЫХ СИСТЕМ “Горизонт-ВС”

Руководство администратора

МБРЦ.468313.002 Д2

Листов 140

Инв. № подл	Подп. и дата	Взам. инв. N	Инв. N дубл.	Подп. и дата

Содержание

Программное изделие (ПИ) “Базовые средства виртуализации вычислительных процессов защищенных операционных систем “Горизонт-ВС” МБРЦ.468313.002 (далее по тексту – ПИ “Горизонт-ВС”) используется для организации исполнения виртуальных машин, а также подключения терминалов к виртуальным машинам (ВМ), исполняемым на сервере виртуализации. ПИ “Горизонт-ВС” устанавливается непосредственно на аппаратное обеспечение в качестве системного программного обеспечения.

В состав ПИ “Горизонт-ВС” входит комплекс программ “Терминал-Сервер” RU.МБРЦ.501130.01-03 (далее по тексту – КП “Терминал-Сервер”) и программа “Система резервирования виртуальных машин” RU.МБРЦ.501290.01-01 (далее по тексту – программа “СРВМ”).

Настоящее руководство является основным документом, описывающим порядок действий администратора при работе с ПИ “Горизонт-ВС”. В руководстве приведены основные сведения, необходимые администратору для установки изделия в вычислительную технику на базе персональных электронных вычислительных машин (ПЭВМ), а также для настройки и эксплуатации изделия.

При эксплуатации изделия необходимо дополнительно руководствоваться документами:

– МБРЦ.468313.002 РЭ. Программное изделие “Базовые средства виртуализации вычислительных процессов защищенных операционных систем “Горизонт-ВС”. Руководство по эксплуатации;

– МБРЦ.468313.002 Д10. Программное изделие “Базовые средства виртуализации вычислительных процессов защищенных операционных систем “Горизонт-ВС”. Руководство по КСЗ;

– МБРЦ.468313.002 Д11. Программное изделие “Базовые средства виртуализации вычислительных процессов защищенных операционных систем “Горизонт-ВС”. Функциональное тестирование.

1 Назначение и основные функции изделия

1.1 Назначение изделия

Изделие предназначено для организации взаимодействия пользователей терминалов с ресурсами серверов виртуализации, объединенных в IP-сеть с использованием технологии “клиент-сервер”.

КП “Терминал-Сервер” является гипервизором, устанавливаемым непосредственно на аппаратное обеспечение в качестве системного программного обеспечения, предназначен для организации исполнения виртуальных машин (ВМ), а также подключения *терминалов* к виртуальным машинам, исполняемым на *сервере виртуализации*, и состоит из двух основных модулей:

– “Тонкий клиент”, который устанавливается на персональные электронные вычислительные машины (ПЭВМ), выполняющие функции терминала (модуль 1 согласно формуляру МБРЦ.468313.002 ФО);

– “Сервер виртуальных машин”, который устанавливается на ПЭВМ, выполняющие функции сервера виртуализации (модуль 2 согласно формуляру МБРЦ.468313.001 ФО).

ПИ “Горизонт-ВС” может применяться для защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, государственных информационных систем (ГИС) до 1 класса защищенности включительно согласно приказу ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации не составляющей государственную тайну, содержащейся в государственных информационных системах» и методическому документу от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах», в информационных системах персональных данных (ИСПДн) до 1 уровня защищенности включительно согласно приказу ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и при построении автоматизированных систем (АС) до 1 класса защищенности включительно согласно приказу ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» в части реализации следующих мер защиты: ИАФ.1, ИАФ.3, ИАФ.4, ИАФ.5, УПД.1, УПД.2, УПД.4, УПД.5, УПД.11, ОПС.3, РСБ.1, РСБ.2, РСБ.3,

РСБ.4, РСБ.5, РСБ.6, РСБ.7, РСБ.8, ОЦЛ.1, ЗСВ.2, ЗСВ.6, ЗСВ.8, ЗИС.1, ЗИС.19, ЗИС.21.

В изделии реализована возможность как локальной работы (на сервере виртуализации), так и на группе серверных платформ (кластере). Управление группой серверов виртуализации осуществляется при помощи системы группового управления (СГУ). Узлы под управлением СГУ разделяются на:

– сервера виртуализации, на которых выполняются ВМ;

– автоматизированные рабочие места (АРМ) управления виртуализацией (АРМ УВ), на которых выполняется СГУ.

Пример схемы стенда с установленными модулями ПИ “Горизонт-ВС” показан на рисунке 1.

Для доступа к СГУ на стенде должно быть подключено АРМ Управления, представляющее собой ПЭВМ с установленной ОС (согласно требованиям п. 1.3.9), в среде которой функционирует браузер.

Локальная работа описана в разделах 2, 4, работа в кластере с СГУ – в разделе 5 настоящего руководства.

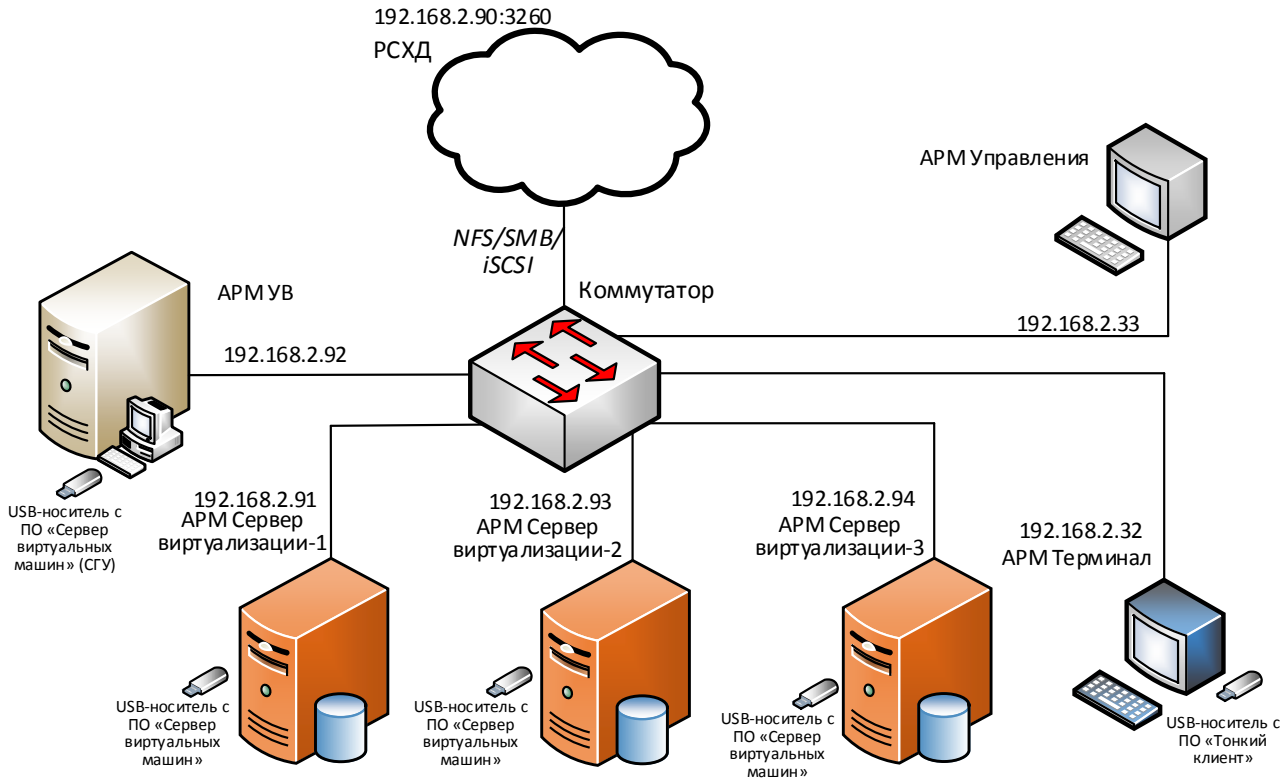


Рисунок 1 – Пример схемы стенда

1.2 Основные функции изделия

1.2.1 Модуль “Тонкий клиент” обеспечивает:

– при работе в административном режиме предоставляет средства для осуществления следующих настроек:
  – настройка сетевых параметров - собственного IP-адреса, маски подсети и IP-адреса шлюза;
  – выбор режима работы терминала - подключение к серверу виртуализации по протоколу SPICE;
  – настройка IP-адреса или полного имени сервера виртуализации и порта для подключения по протоколу SPICE;
  – настройка параметров соединения терминала с сервером виртуализации;
– подключение по протоколу SPICE к ВМ, исполняемым на сервере виртуализации;
– вывод графической и звуковой информации ВМ через терминал;
– ввод информации с клавиатуры терминала в ВМ;
– подключение манипулятора типа "мышь" (далее по тексту - мышь") терминала к ВМ;
– ввод звуковой информации в ВМ через микрофон терминала;
– подключение USB v1.1 и v2.0 устройств терминала к ВМ;
– восстановление системы после сбоя;
– непрерывную круглосуточную работу.

1.2.2 Модуль “Сервер виртуальных машин” обеспечивает:

– возможность создания и исполнения виртуальных машин (ВМ);
– возможность создания и редактирования виртуального аппаратного окружения ВМ;
– запуск, остановку, перезагрузку, приостановку, клонирование, создание копии состояния и удаления ВМ;
– поддержку работы 32- и 64-битных гостевых операционных систем (ОС) под управлением ОС семейства Windows и Linux
– мониторинг виртуальных машин;
– создание и редактирование виртуальных сетей;
– возможность создания и редактирования виртуальных сетевых мостов;
– доверенное подключение терминалов к ВМ, исполняемым на сервере виртуализации;
– миграцию виртуальных машин;

– создание "снимков" работающих виртуальных машин;

– тестирование всех функциональных блоков;

– протоколирование сбойных ситуаций;

– восстановление системы после сбоя;

– непрерывную круглосуточную работу;

– использование веб-интерфейса для управления виртуальной инфраструктурой;

– создание и управление виртуальной инфраструктурой с поддержкой кластеризации;

– создание и хранение образов ВМ для их развёртывания;

– создание шаблонов ВМ;

– подключение общих хранилищ по протоколам NFS/SMB;

– использование хранилищ, подключаемых по протоколу iSCSI, в качестве общих хранилищ;

– создание, подключение/отключение от ВМ, клонирование, уничтожение виртуальных дисков;

– обеспечение возможности запуска ВМ в режиме высокой доступности;

– функционирование видеокарт с GPU (проброс аппаратной части в ВМ);

– независимую обработку входящей и исходящей информации по меткам, связанным с категорией информации;

– возможности мониторинга по протоколу SNMP (RFC 3411) всех компонент виртуальной инфраструктуры.

Комплекс программ “Терминал-Сервер” обеспечивает защиту обрабатываемой информации, содержащей сведения, составляющие государственную тайну, от несанкционированного доступа (НСД), включая:

– идентификацию и аутентификацию пользователей;

– дискреционный принцип контроля доступа;

– мандатный принцип контроля доступа;

– очистку оперативной и внешней памяти;

– изоляцию модулей;

– маркировку документов;

– защиту ввода и вывода на отчуждаемый физический носитель информации;

– сопоставление пользователя с устройством;

– регистрацию событий защиты;

– взаимодействие пользователя с комплексом средств защиты (КСЗ);

– надежное восстановление свойств КСЗ;

– контроль целостности программных файлов и данных;

– тестирование изделия;

– защиту среды виртуализации.

1.2.3 Программа “СРВМ” обеспечивает:

– периодическое сохранение конфигураций ВМ, исполняемых на сервере виртуализации;

– периодическое сохранение дисков ВМ, исполняемых на сервере виртуализации;

– периодическое сохранение конфигураций "снимков" работающих ВМ, исполняемых на сервере виртуализации;

– периодическое сохранение конфигураций виртуальных сетей, работающих на сервере виртуализации;

– отображение информации о времени создания и актуальности резервных копий конфигураций ВМ, дисков ВМ, конфигураций "снимков" работающих ВМ, а также виртуальных сетей;

– управление частотой обновления резервных копий конфигураций ВМ, дисков ВМ, конфигураций "снимков" работающих ВМ, а также виртуальных сетей.

1.3 Указания по эксплуатации

1.3.1 Изделие соответствует требованиям МБРЦ.468313.002 ТУ при соблюдении следующих требований к аппаратной платформе:

а) наличие интерфейса USB 1.1, 2.0;

б) оперативная память не менее 4 Гб для сервера виртуализации и не менее 256 Мб для терминала;

в) процессор класса x86 не ниже Pentium 4 для терминала и с поддержкой технологии Intel-VT или AMD-V для сервера виртуализации;

г) жесткий диск не менее 100 Гб для сервера;

д) наличие разъема SATA на материнской плате.

1.3.2 Установка изделия и последующая эксплуатация производятся в соответствии с руководством администратора МБРЦ.468313.002 Д2 и руководством по эксплуатации МБРЦ.468313.002 РЭ.

1.3.3 После установки и настройки изделия в обязательном порядке должна быть исключена возможность бесконтрольного доступа к носителям изделия, размещенным в системном блоке ПЭВМ.

1.3.4 Технические средства ПЭВМ, в которую устанавливается носитель с изделием, не должны содержать аппаратно-программных механизмов, ориентированных на целенаправленное нарушение правильности его функционирования.

1.3.7 В изделии на одной ВМ может быть зарегистрирован только один уникальный пользователь.

1.3.8 Журналы регистрации событий, имеющие отношение к безопасности, должны иметь в своих записях точное указание даты и времени.

1.3.9 Установка пароля для графического сервера Spice обязательна согласно п. 3.7.9;

1.3.10 Гостевые ОС, устанавливаемые в ВМ, должны иметь сертификат соответствия не ниже 3 класса защищенности от НСД и не ниже 2 уровня контроля отсутствия недекларированных возможностей (НДВ).

1.3.11 Периодический контроль целостности обеспечивается периодической перезагрузкой *сервера виртуализации* и *терминалов*.

1.3.12 Контроль целостности USB-накопителей с ПИ “Горизонт-ВС” производится путем вычисления контрольных сумм файлов согласно процедуре, описанной в формуляре МБРЦ.468313.002 ФО (Приложение А) и сверки полученных значений с указанными в формуляре. Данную процедуру необходимо проводить перед каждым запуском *сервера виртуализации* и *терминалов*.

1.3.13 В ПИ “Горизонт-ВС” реализована изолированная программная среда, в которой установлен КП “Терминал-Сервер”, под управлением которого ведется работа, а также установлена его неизменность для определенного сеанса работы. С целью предотвращения нарушения целостности замкнутой среды ПИ “Горизонт-ВС” на действия суперпользователя *root* накладываются ограничения. Администратор с правами суперпользователя может выполнять следующие действия:

1. Вносить изменения в конфигурационные файлы, расположенные в директориях ***/etc/auditd/*** и ***/etc/libvirt/.***

2. Просматривать все файлы системы с использованием всех доступных системных утилит и средств фильтрации.

3. Использовать любые системные утилиты без внесения изменений в системные файлы и файлы конфигураций.

ВНИМАНИЕ: 1 ЗАПРЕЩЕНЫ ДЕЙСТВИЯ, СВЯЗАННЫЕ С ИЗМЕНЕНИЕМ КОНФИГУРАЦИОННЫХ ФАЙЛОВ, НЕ УКАЗАННЫХ В П.1 И ЗАПУСКОМ, ОТКЛЮЧЕННЫХ ПО УМОЛЧАНИЮ СЕРВИСОВ (НАПРИМЕР, SSH).

2 ЗАПРЕЩЁН ЗАПУСК ВМ ИЗ МЕНЕДЖЕРА ВИРТУАЛЬНЫХ МАШИН.

4. Задавать в файле sudoers, расположенном в директории ***/etc***, команды, которые может выполнять администратор (vss).

Структура файла может иметь следующий вид:

Cmnd_Alias PROCESSES = /bin/kill, /usr/bin/top, /sbin/service, /sbin/ausearch, /sbin/aureport, /bin/cat, /bin/grep, /usr/bin/tail

root ALL=(ALL) ALL

vss ALL=NOPASSWD: PROCESSES

В строке *PROCESSES* перечисляются процессы, которые доступны для запуска администратором из консоли.

2 Установка ПИ “Горизонт-ВС”

В данном разделе описана процедура установки ПИ “Горизонт-ВС” на серверы виртуализации и АРМ управления виртуализацией.

2.1 Включение сервера виртуализации

Так как КП “Терминал-Сервер” поставляется на USB-носителе, то перед включением сервера виртуализации необходимо подключить съемный USB-носитель с установленным программным обеспечением КС в один из свободных USB-разъемов на сервере. После этого следует включить питание сервера. Далее необходимо зайти в BIOS и установить в качестве основного загрузочного устройства подключенный USB-накопитель.

Примечание. Для того чтобы войти в BIOS, в начале загрузки компьютера необходимо нажать специальную клавишу (например, **Del** или **F2**), когда на экране появится сообщение, предлагающее это сделать. Чаще всего можно встретить сообщения следующего вида: “**Press DEL to enter Setup**”, или “**Press F2 to access the BIOS**”.

После сохранения настроек и перезагрузки сервера на мониторе будет отображаться процесс загрузки ПИ “Горизонт-ВС”. После завершения процесса тестирования всех функциональных блоков на экране появится окно аутентификации (рисунок 6).

Рисунок 2 - Окно аутентификации

В данном окне следует нажать на строку ***Ещё***, ввести имя суперпользователя **root**, пароль по умолчанию **horizon** и нажать клавишу **Enter** – загрузится рабочий стол ПИ “Горизонт-ВС”.

2.2 Установка ПИ “Горизонт-ВС” на сервер виртуализации

Для установки ПИ “Горизонт-ВС” на жесткий диск сервера виртуализации требуется зайти в меню *Приложения->Системные->Редактор разделов*, после чего откроется окно **GParted** (рисунок 14).

В окне **Редактор разделов** во второй строке меню справа из раскрывающего списка следует выбрать жесткий диск, на который будет производиться установка ПИ “Горизонт-ВС”. После этого выбранный диск и его свойства появятся в нижней части окна.

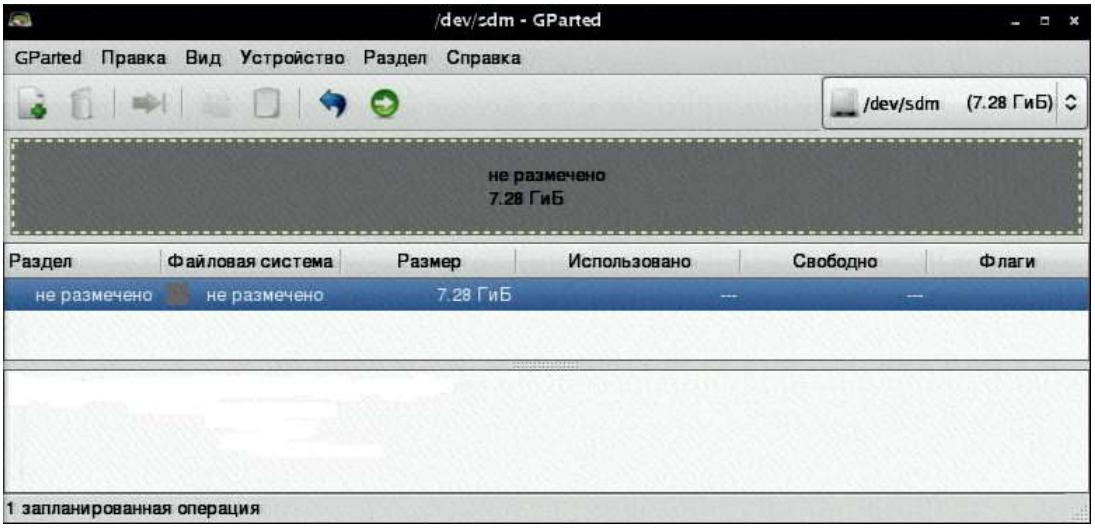


Рисунок 3 - Окно управления дисковыми устройствами

Далее необходимо нажать правой кнопкой манипулятора типа “мышь” (далее по тексту - “мышь”) в неразмеченную область диска и в открывшемся меню выбрать пункт **Новый** – на экране появится окно **Создать новый раздел** (рисунок 15).

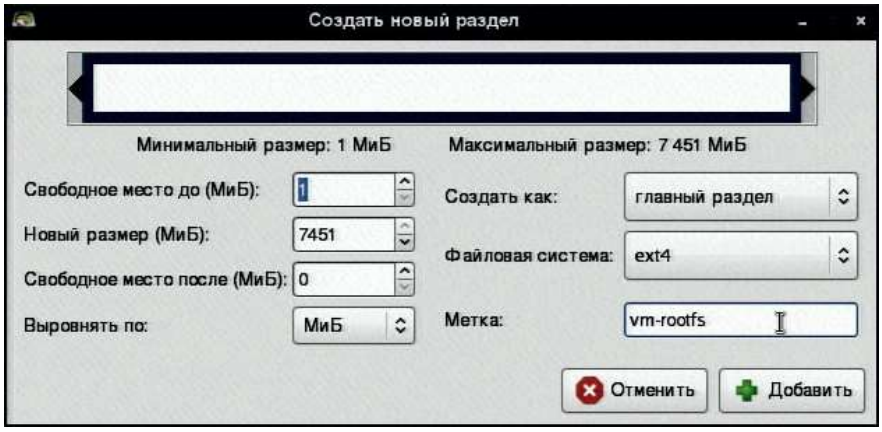


Рисунок 4 - Создать новый раздел

Следует ввести необходимый размер нового раздела, в поле **Создать как** выбрать пункт ***главный раздел***, файловую систему выбрать ***ext4*** и указать метку ***vm-rootfs***, после чего нажать кнопку **Добавить**.

В окне **GParted** (рисунок 14) нужно нажать кнопку “**Применить все операции**”

, после этого запустится процесс создания нового раздела (рисунок 16).

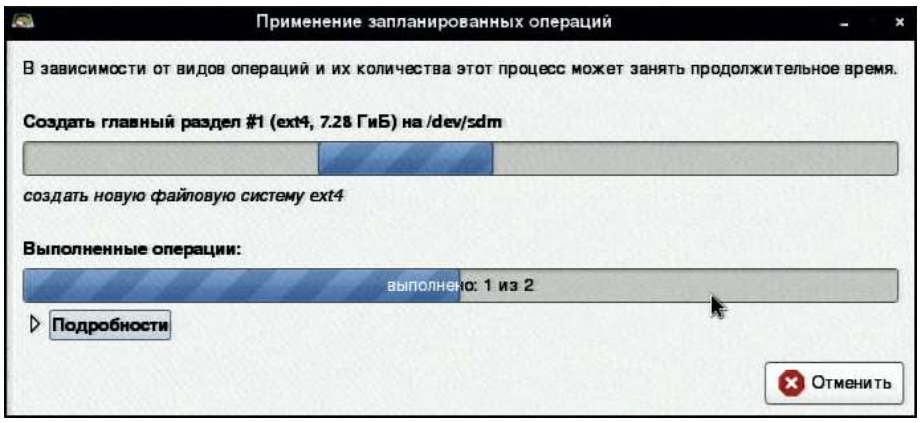


Рисунок 5 - Применение запланированных операций

После завершения применения операций необходимо перезагрузить сервер, для того чтобы ПО установилось на настроенный раздел. При дальнейшей работе загрузка ПИ “Горизонт-ВС” производится с USB-носителя, на котором размещен неизменяемый образ, после загрузки USB-носитель можно извлекать из системного блока *сервера виртуализации*.

2.3 Установка ПИ “Горизонт-ВС” на АРМ УВ

Установка СГУ на *АРМ УВ* осуществляется следующим образом.

Необходимо установить ПИ “Горизонт-ВС” на жесткий диск так, как описано в п.п. 2.1, 2.2. Далее следует запустить СГУ командой в консоли:

 # service one start

и запустить сервис SSH командой:

 # service sshd start

Дальнейшая работа возможна из браузера *АРМ управления* указанием ip-адреса *АРМ УВ* и порта 9869 (например, *192.168.1.10:9869*). Логин и пароль для входа в СГУ «**admin/admin**».

Примечание: если ip-адрес *АРМ УВ* был получен по DHCP, его можно узнать командой: ***# ifconfig sys0***

Подробная работа с СГУ описана в разделе 5 настоящего руководства.

2.4 Первоначальные настройки сервера виртуализации

Работа ПИ “Горизонт-ВС” может осуществляться как в режиме одиночного гипервизора, так и группы серверов виртуализации. Порядок работы с группой гипервизоров при помощи системы группового управления (СГУ) описан в п. 5.

После установки ПИ “Горизонт-ВС” на серверах виртуализации и АРМ УВ необходимо произвести следующие настройки от имени суперпользователя *root*:

1. Если платформа будет выполнять функции *сервера виртуализации*, то следует отключить СГУ командой в консоли: **service one stop**.
2. Сменить пароль администратора vss (п. 3.1.1)
3. Настроить ip-адрес сервера виртуализации (п. 3.3) или произвести настройку виртуального коммутатора (п. 3.10).
4. При необходимости осуществить разметку дисковой подсистемы при помощи утилиты **GParted**, входящей в состав ПИ «Горизонт-ВС» (п. 3.2).
5. Настроить мандатные категории (п. 3.5).
6. При помощи Менеджера пользователей ВМ (п. 3.4) создать специального пользователя с именем “*server_view_<порядковый номер сервера>*”.
7. Заполнить файл в директории ***/etc/vmacd/hvs***, содержащий список всех серверов виртуализации и резервирования, входящих в группу, в следующем формате:

IP-адрес сервера;имя_пользователя@horizon;пароль

где IP-адрес сервера – адрес сервера виртуализации или резервирования;
имя_пользователя – имя ранее специально созданного пользователя, который будет использоваться службой vmacd для получения данных о состоянии ВМ от службы libvirtd;
пароль – пароль, назначенный специальному пользователю.

Примечания:

1) Рекомендуемый размер группы – до 255 гипервизоров.

2) Файл ***/etc/vmacd/hvs*** должен заканчиваться символом перевода строки.

3) Файл ***/etc/vmacd/hvs*** необходимо редактировать на всех серверах виртуализации и резервирования, входящих в группу, при изменении параметров этих серверов (IP-адрес или данные пользователя).

4) Следует установить права доступа на файл ***/etc/vmacd/hvs*** только для суперпользователя root командой в консоли: ***chmod 600 /etc/vmacd/hvs.***

8. После заполнения файла ***/etc/vmacd/hvs*** необходимо перезапустить сервис vmacd командой в консоли: **service vmacd restart**.
9. Установить разрешение доступа к серверу SAMBA командой в консоли: **chmod 04755 /usr/sbin/samba**.
10. Удалить ссылку командой в консоли: **rm –f /usr/libexec/qemu-kvm**.
11. Перезагрузить *сервер виртуализации*.

3 Работа администратора с сервером виртуализации

3.1 Запуск сервера виртуализации

Загрузка ПИ “Горизонт-ВС” производится с USB-носителя, на котором размещен неизменяемый образ системы. В процессе загрузки производится расчет контрольных сумм неизменяемой части корневой файловой системы, установленной на жесткий диск *сервера виртуализации*, и их сравнение с контрольными суммами файлов на USB-носителе. В случае полного соответствия вычисленных контрольных сумм эталонным система продолжает загрузку, после окончания которой USB-носитель можно извлекать из системного блока *сервера виртуализации*. В противном случае загрузочный скрипт осуществляет безусловное копирование неизменяемой корневой части файловой системы с USB-носителя.

3.1.1 Вход в систему

После загрузки ПИ “Горизонт-ВС” на экране появится окно аутентификации (рисунок 6).

Рисунок 6 - Окно аутентификации

В данном окне следует ввести необходимое имя администратора, пароль и нажать клавишу **Enter** – загрузится рабочий стол ПИ “Горизонт-ВС”.

Примечание. По умолчанию на предприятии-изготовителе устанавливаются следующие параметры:

- администратор – логин **vss**, пароль отсутствует;
- суперпользователь – логин **root**, пароль **horizon**.

После первой загрузки необходимо сменить пароль администратора от имени суперпользователя root командой в консоли ***passwd vss***. После чего следует дважды корректно ввести новый пароль.

3.1.2 Графические средства администрирования

Для администрирования изделия используется меню “Приложения”, расположенное в левом нижнем углу экрана (рисунок 7).

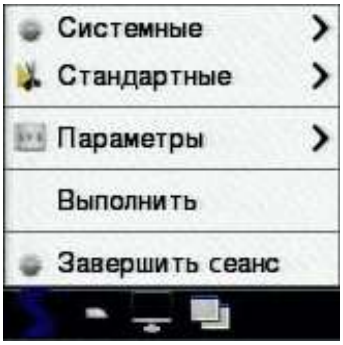


Рисунок 7 - Меню "Приложения"

Меню состоит из трех раскрывающихся подпунктов (**Системные, Стандартные, Параметры**), каждый из которых открывает доступ к настройкам соответствующей области, команды **Выполнить**, позволяющей получить быстрый доступ стандартным приложениям и настройкам, а также команды **Завершить сеанс**, обеспечивающей корректное завершение работы системы.

3.1.2.1 Приложения->Системные

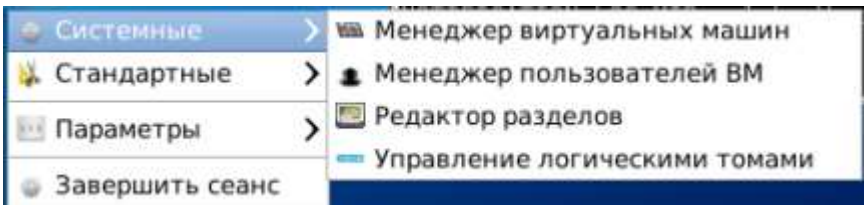


Рисунок 8 - Меню "Системные"

Подменю **Системные** (рисунок 8) состоит из трех подразделов:

- **GParted** – программа для управления дисковыми устройствами (подробнее см. раздел 3.2 настоящего руководства);
- **Менеджер виртуальных машин** – программа для работы с виртуальными машинами и виртуальными сетями (подробнее см. раздел 3.5 настоящего руководства);
- **Менеджер пользователей виртуальных машин** – программа для работы со списком пользователей виртуальных машин (подробнее см. раздел 3.4 настоящего руководства);
- **Управление логическими томами** – программа, предоставляющая возможность управления хранилищами данных.

3.1.2.2 Приложения->Стандартные

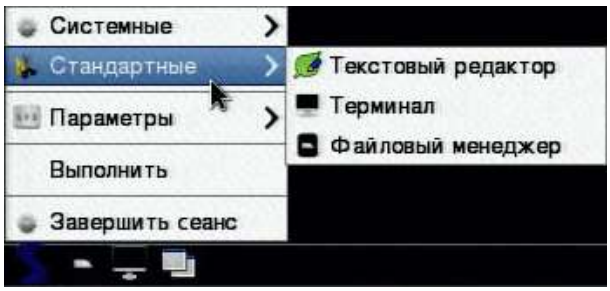


Рисунок 9 - Меню "Стандартные"

Из подменю **Стандартные** (рисунок 9) можно запустить следующие программы:

- **“Текстовый редактор”** для создания и редактирования текстовых документов;
- **“Терминал”** консоль для выполнения управляющих команд;
- **“Файловый менеджер”** для работы с файловой системой.

3.1.2.3 Приложения->Параметры

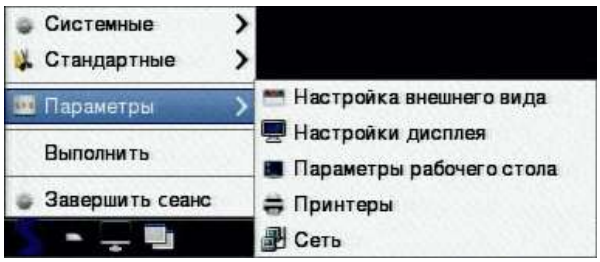


Рисунок 10 - Меню "Параметры"

Из подменю **Параметры** (рисунок 10) можно запустить следующие программы:

- **“Настройка внешнего вида”** (рисунок 11) для выбора цветовой темы окон, вида значков, курсора и шрифтов элементов интерфейса.

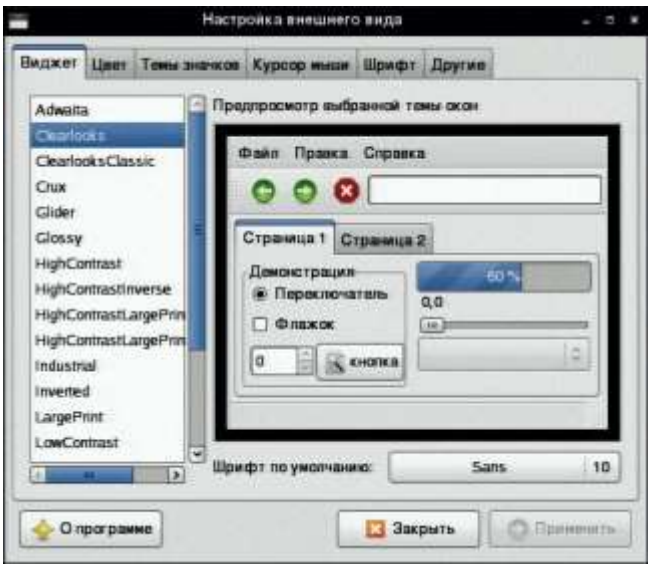


Рисунок 11 - Настройка внешнего вида

- **“Настройки дисплея”** (рисунок 12) для задания параметров изображения на мониторе.

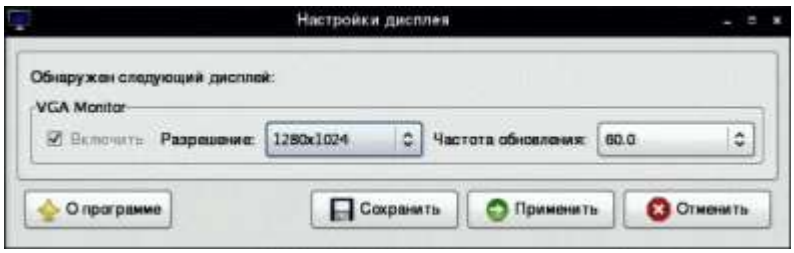


Рисунок 12 - Настройки дисплея

- **“Параметры рабочего стола”** (рисунок 13) для изменения оформления рабочего стола и текста ярлыков.

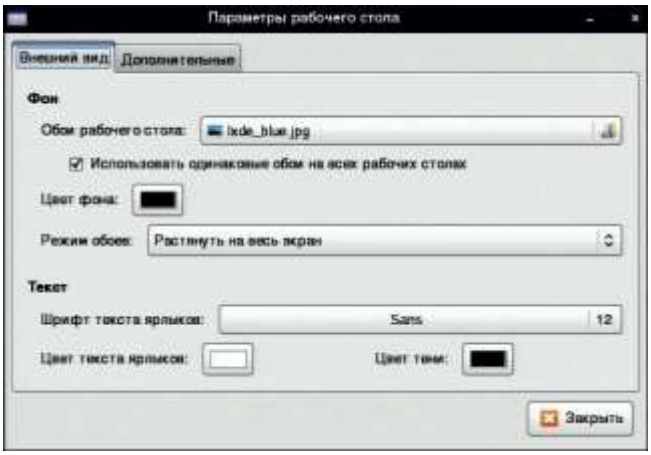


Рисунок 13 - Параметры рабочего стола

- **“Принтеры”** для подключения принтеров к серверу виртуализации (подробнее см. раздел 3.10 настоящего руководства).
- **“Сеть”** для настройки сетевых устройств (подробнее см. раздел 3.3 настоящего руководства).

3.2 Настройка дисковых разделов ПИ “Горизонт-ВС”

Для установки системы требуется зайти в меню *Приложения->Системные->Редактор разделов*, после чего откроется окно **Редактор разделов** (рисунок 14).

В окне **Редактор разделов** во второй строке меню справа из раскрывающего списка следует выбрать жесткий диск, на который будет производиться установка ПО “Горизонт-ВС”. После этого выбранный диск и его свойства появятся в нижней части окна.

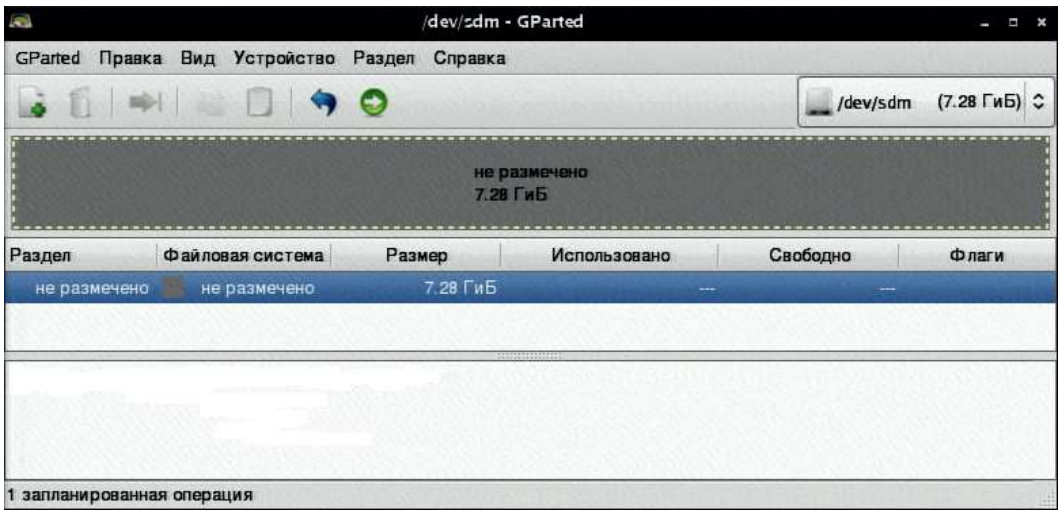


Рисунок 14 - Окно управления дисковыми устройствами

Далее необходимо нажать правой кнопкой манипулятора типа “мышь” (далее по тексту - “мышь”) в неразмеченную область диска и в открывшемся меню выбрать пункт **Новый** – на экране появится окно **Создать новый раздел** (рисунок 15).

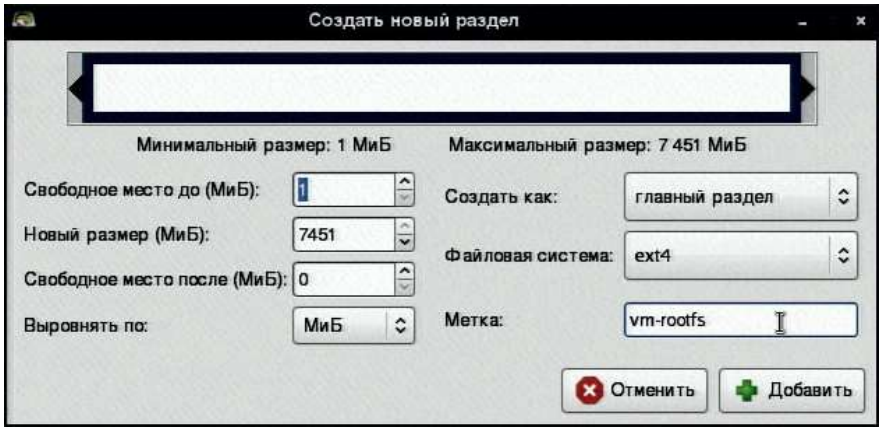


Рисунок 15 - Создать новый раздел

Следует ввести необходимые данные о разделе, после чего нажать кнопку **Добавить**. В окне **Редактор разделов** (рисунок 14) нужно нажать кнопку “**Применить все операции**”, после этого запустится процесс создания нового раздела (рисунок 16).

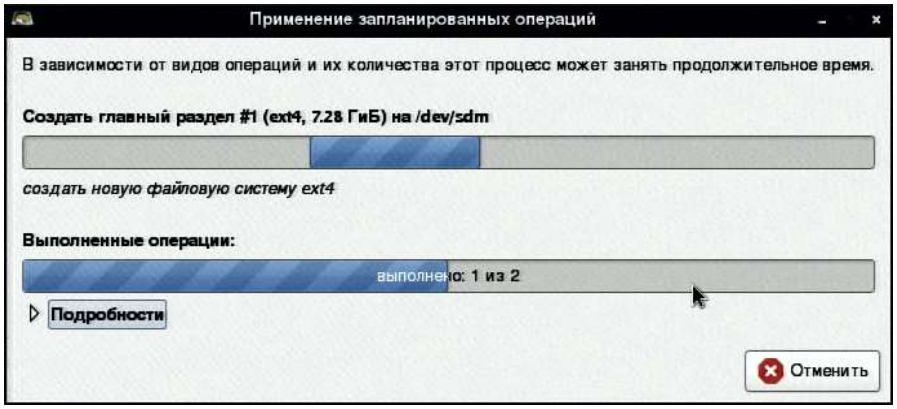


Рисунок 16 - Применение запланированных операций

3.3 Настройка сети

Для настройки сетей необходимо зайти в меню *Приложения->Параметры-> Сеть*, после чего откроется окно **Настройка сети** (рисунок 17).

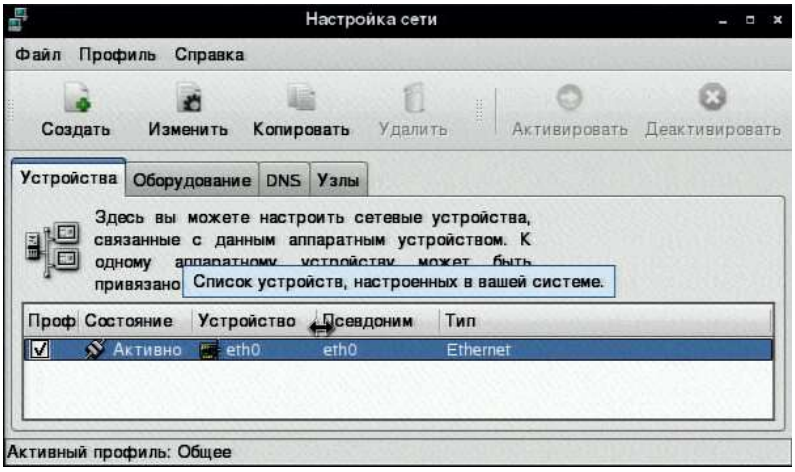


Рисунок 17 – Настройка сети

3.3.1 Вкладка “Устройства”

На вкладке **Устройства** (рисунок 17) приведен список сетевых устройств, связанных с подключенными к серверу аппаратными устройствами.

Для редактирования настроек устройства, необходимо выбрать его в списке и нажать кнопку **Изменить**.

Для того чтобы добавить новое устройство, необходимо нажать кнопку **Создать** – запустится процесс создания нового соединения:

1. На первом шаге следует из списка в левой части окна выбрать тип нового соединения (рисунок 18) и для продолжения нажать кнопку **Вперед**.

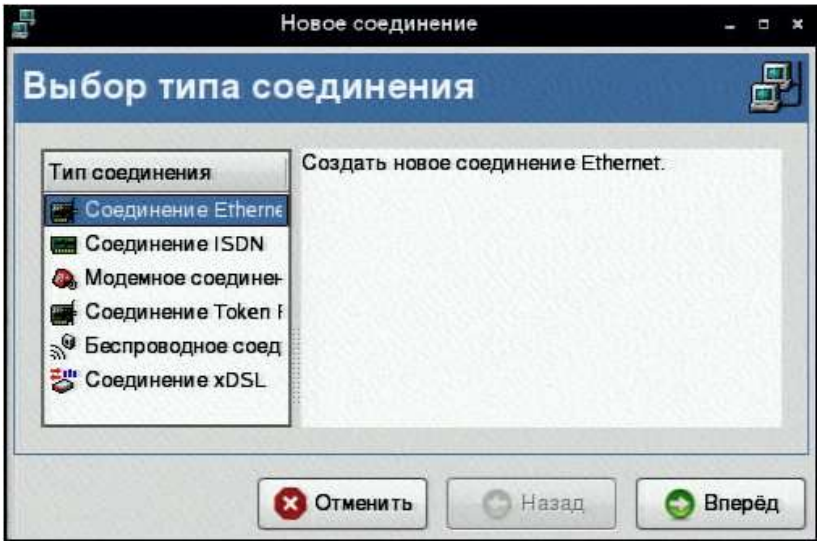


Рисунок 18 – Выбор типа соединения

2. Далее необходимо выбрать аппаратное устройство (рисунок 19).

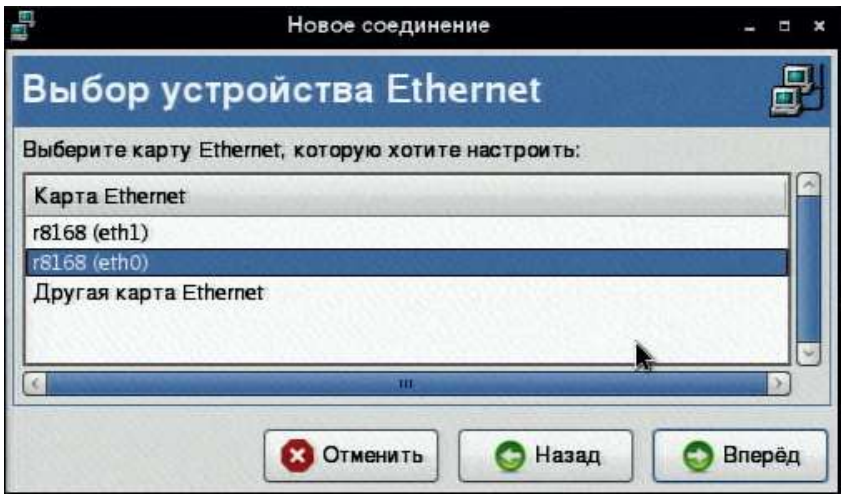


Рисунок 19 – Выбор устройства

3. На следующем шаге следует ввести адрес IP, DNS серверов и при необходимости установить флажок **Задать MTU** (величину максимальной единицы передачи) и выбрать ее значение из списка (рисунок 20).

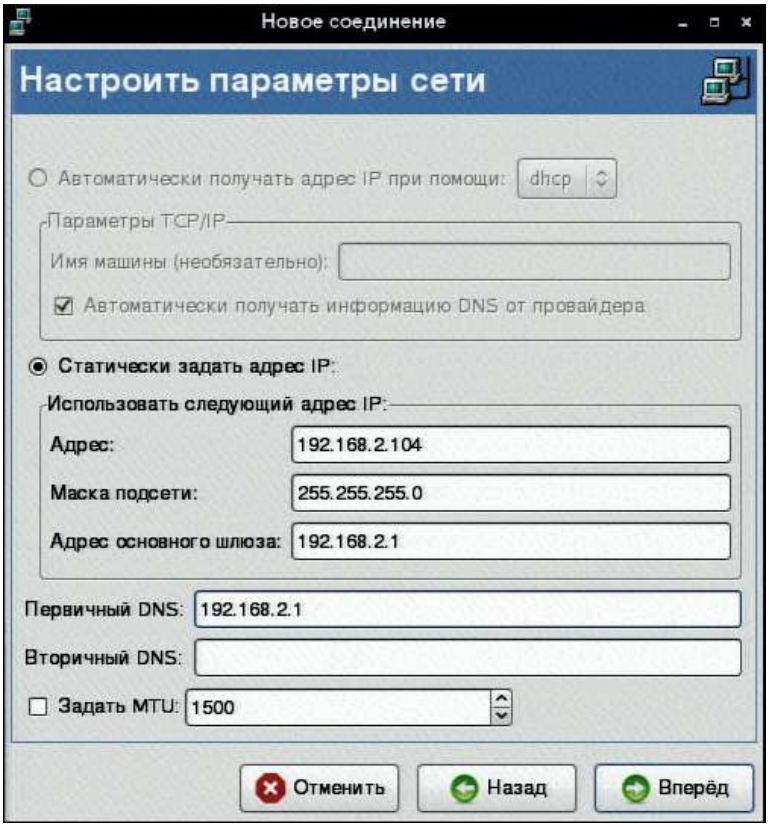


Рисунок 20 – Настройка параметров сети

4. Далее следует проверить введенную информацию, при необходимости внести изменения путем нажатия кнопки **Назад**, а чтобы завершить создание нового устройства, нажать кнопку **Применить** (рисунок 21).

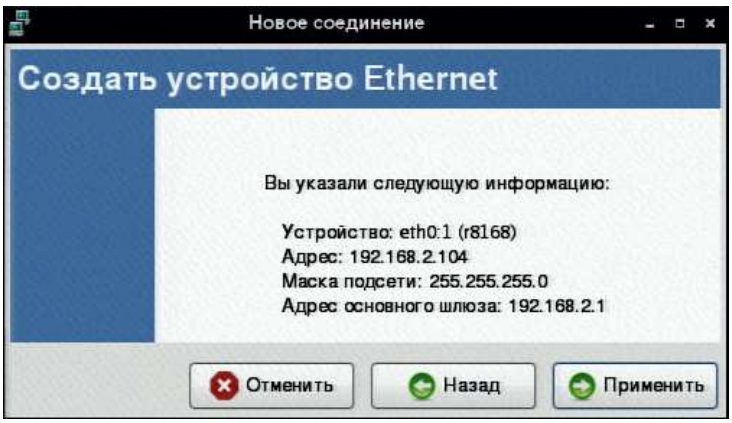


Рисунок 21 – Проверка информации

5. После этого в окне **Настройка сети** (рисунок 17) выбрать в меню команду *Файл->Сохранить*.

3.3.2 Вкладка “Оборудование”

На вкладке **Оборудование** (рисунок 22) приведен список оборудования, физически подключенного к серверу виртуализации.

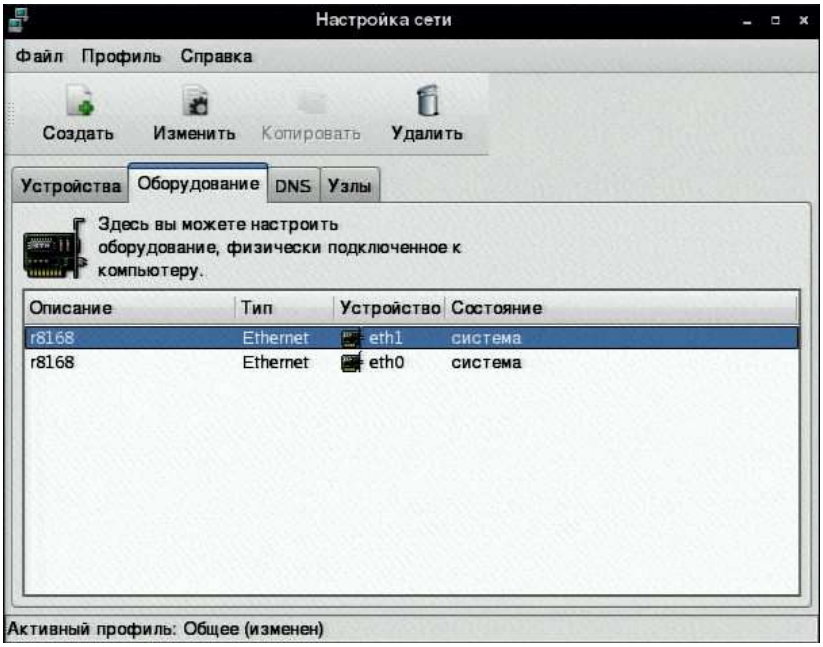


Рисунок 22 – Настройка сети. Вкладка «Оборудование»

Для редактирования настроек оборудования необходимо выбрать его в списке и нажать кнопку **Изменить**. Для удаления оборудования следует выбрать его в списке и нажать кнопку **Удалить**.

Для того чтобы добавить новое устройство, необходимо нажать кнопку **Создать**, после чего откроется окно (рисунок 23), в котором следует выбрать тип устройства.

Рисунок 23 – Выбор типа оборудования

Далее необходимо выбрать сетевой адаптер и тип устройства и нажать кнопку **ОК** (рисунок 24) – добавленное оборудование появится в списке.

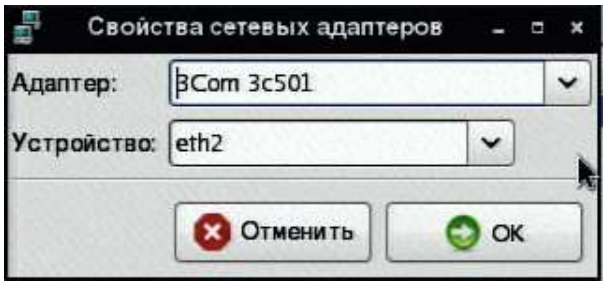


Рисунок 24 – Свойства сетевых адаптеров

3.3.3 Вкладка “DNS”

На вкладке **DNS** (рисунок 25) можно настроить имя компьютера, домен, сервера имен и домен поиска.

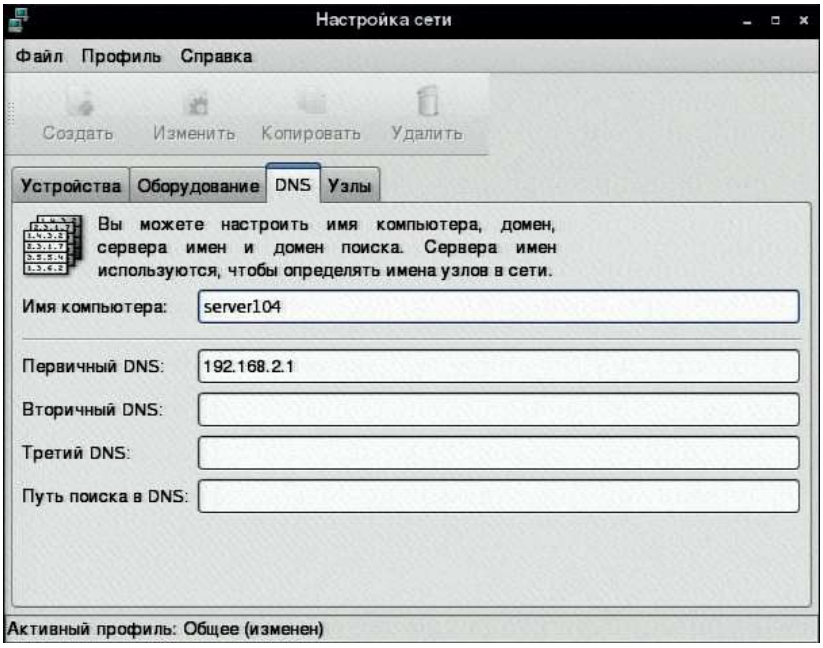


Рисунок 25 – Настройка сети. Вкладка «DNS»

3.3.4 Создание замкнутой изолированной вычислительной среды

Для создания изолированной вычислительной среды необходимо запретить весь входящий и исходящий трафик следующими командами:

 # iptables -P INPUT DROP

 # iptables -P OUTPUT DROP

 # iptables -P FORWARD DROP

 # iptables -L -v -n

3.4 Создание и удаление пользователей

С каждым пользователем ПИ “Горизонт-ВС” связан уникальный идентификатор – идентификатор пользователя (UID), который используется для определения прав доступа. Каждая ВМ на сервере виртуализации запускается с UID запустившего ВМ пользователя. При обращении ВМ к объекту (файлу) доступ предоставляется по результатам процедуры авторизации, то есть обработки запроса на основе дискреционных и мандатных правил разграничения доступа (ПРД).

Для работы с пользователями виртуальных машин следует зайти в меню *Приложения-> Системные->Менеджер пользователей виртуальных машин* (или набрать команду в консоли ***vs-users***), после чего откроется окно **Менеджер пользователей ВМ** (рисунок 26).

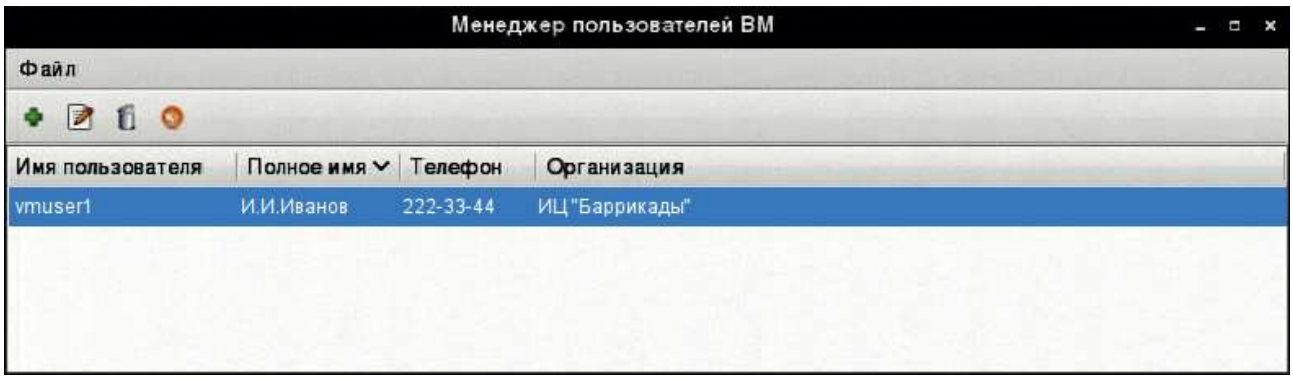


Рисунок 26 - Менеджер пользователей ВМ

В верхней части окна находится управляющее меню, в нижней – список зарегистрированных пользователей в системе.

Для *создания* нового пользователя необходимо нажать кнопку в управляющем меню – откроется окно **Новый пользователь ВМ** (рисунок 27).

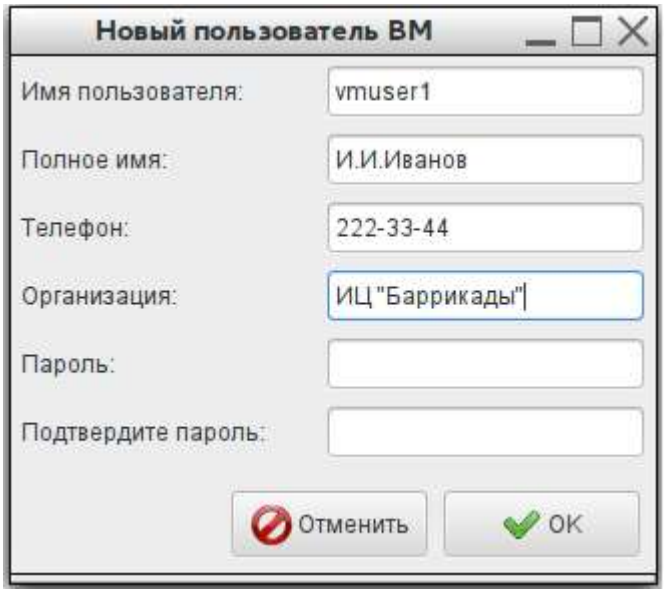


Рисунок 27 – Новый пользователь ВМ

В открывшемся окне следует ввести следующие данные:

– **имя пользователя** – имя пользователя, как оно будет отображаться в системе;

– **полное имя** – ФИО пользователя;

– **телефон** – контактный телефон пользователя;

– **организация** – наименование организации, к которой принадлежит пользователь;

– **пароль** и **подтвердить пароль** – пароль пользователя.

После заполнения всех полей нужно нажать кнопку ОК (рисунок 27), и в главном окне (рисунок 26) в списке появится новый пользователь.

После создания пользователя необходимо перезапустить сервисы libvirtd и vmacd командами в консоли:

service libvirtd restart

service vmacd restart

Примечания:

1) если будет назначен слишком простой пароль, то на экране появится предупреждающее сообщение (рисунок 28). Для подтверждения пароля следует нажать кнопку **Да**, для коррекции пароля – кнопку **Нет**.

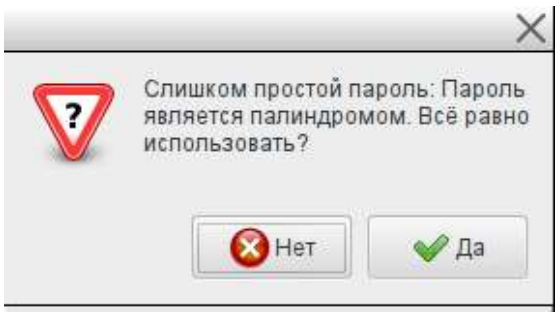


Рисунок 28 - Сообщение

2) имя пользователя должно быть уникальным. Если будет введено имя, уже существующее в системе, то на экране появится предупреждающее сообщение (рисунок 29).

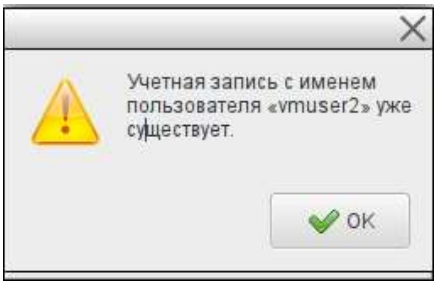


Рисунок 29 - Сообщение

Для *редактирования* существующего пользователя администратору необходимо выделить в списке (рисунок 26) нужного пользователя и нажать кнопку  в управляющем меню – откроется окно **Редактировать пользователя ВМ** (рисунок 30).

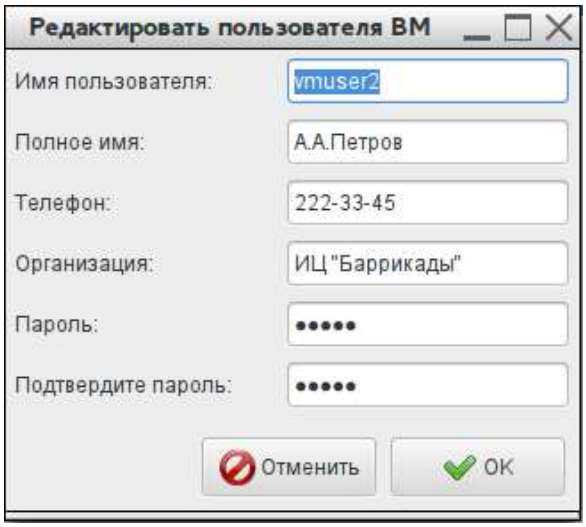


Рисунок 30 - Редактирование пользователя ВМ

В открывшемся окне возможно редактировать ранее введенную информацию о пользователе ВМ.

Для *удаления* пользователя необходимо выделить в списке (рисунок 26) нужного пользователя и нажать кнопку  в управляющем меню – появится предупреждающее сообщение (рисунок 31).

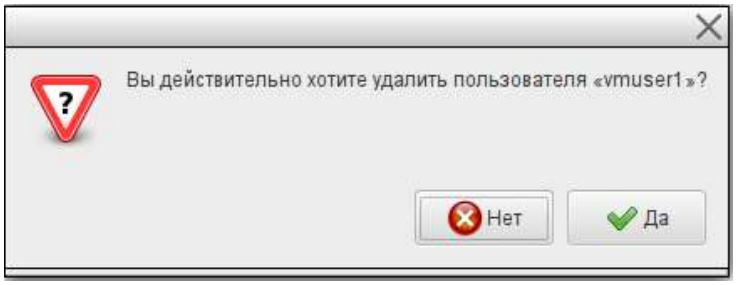


Рисунок 31 - Предупреждающее сообщение

Для подтверждения удаления следует нажать кнопку **Да**, после чего пользователь будет удален; для отмены действия следует нажать кнопку **Нет**.

Примечания:

1 после удаления пользователя владелец всех файлов в директории ***/srv/samba***, принадлежащих удаляемому пользователю, изменяется на root.

2 после обновления списка пользователей необходимо перезапустить сервис vmacd командой в консоли: ***service vmacd restart***.

Назначение пользователю ВМ описано в разделе 3.7.1 настоящего руководства.

3.5 Создание мандатных и дискреционных категорий

В ПИ “Горизонт-ВС” реализован мандатный и дискреционный принцип контроля доступа, которые обеспечивает управление доступом путем сопоставления меток безопасности каждого субъекта (пользователя) и каждого объекта (файла).

3.5.1 Создание мандатных меток

Метки безопасности задаются только администратором root и могут быть скорректированы им в процессе работы.

Создание уровней доступа в системе осуществляется в файле *translate*, находящемся в директории ***/etc/smack***. Пример файла приведен на рисунке 32.

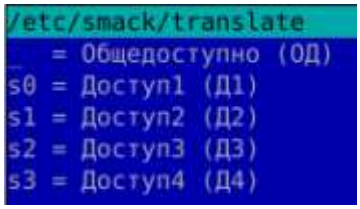


Рисунок 32 - Пример файла translate

Данные вносятся в следующем порядке:

<метка> = <длинное название уровня доступа> (<короткое название>)

Создаваемые метки должны быть уникальными и отражать смысловую нагрузку уровней доступа. Метка самого нижнего уровня доступа обозначается символом “_”. Наличие всех полей обязательно.

Схема мандатного доступа задается в файле *acceses*, находящемся в директории ***/etc/smack***. Пример заполнения файла приведен на рисунке 33.

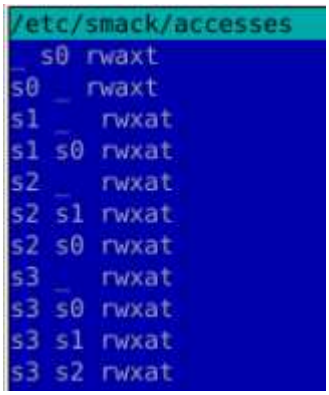


Рисунок 33 - Пример файла accesses

Данные заполняются строго в следующем порядке:

- первая колонка – субъект доступа;
- вторая колонка – объект доступа;

- третья – права доступа (возможные значения: r – чтение, w – запись, x – исполнение, a – дополнение, t – удалить файл может только владелец этого файла).

Например, первую строку можно расшифровать как “субъект с меткой общедоступно имеет доступ к объектам с меткой S0 на все виды доступа”.

Созданные уровни доступа назначаются на ВМ в поле **Уровень доступа** подменю “Обзор” (п. 3.7.1). Так как по регламенту к ВМ имеет доступ только один пользователь

3.5.2 Назначение дискреционных прав доступа

По умолчанию после создания файла на хранилище SAMBA на него назначаются дискреционные права полного доступа для владельца и запрет доступа для группы и других пользователей.

Смена дискреционных прав доступа к файлам осуществляется при помощи команд **chmod** и **chown**. Описание работы с хранилищем SAMBA приведено в п. 3.12 данного руководства.

Команда **chown** изменяет владельца и/или группу для каждого заданного файла.

В качестве имени владельца/группы берется первый аргумент, не являющийся опцией. Если задано только имя пользователя (или UID 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.

Для изменения владельца файла следует в консоли набрать команду вида:

chown *[опции] имя_пользователя[:группа] имя_файла*

Для команды доступны следующие опции:

- -c, --changes – подробно описывать действие для каждого файла, владелец которого действительно изменяется.
- -f, --silent, --quiet – не выдавать сообщения об ошибках для файлов, чей владелец не может быть изменен.
- -h, --no-dereference – работать с самими символьными ссылками, а не с файлами, на которые они указывают. Данная опция доступна только если имеется системный вызов lchown.
- -v, --verbose – подробное описание действия (или отсутствия действия) для каждого файла.
- -R, --recursive – рекурсивное изменение владельца каталогов и их содержимого.

Для вызова описания команды и примеров следует набрать команду в консоли ***chown --help***.

Команда **chmod** изменяет права доступа к файлам и директориям:

chmod [опции] режим файл

Команда изменяет права доступа каждого указанного *файла* в соответствии с правами доступа, указанными в параметре *режим*, который может быть представлен как в символьном виде, так и в виде восьмеричного числа, представляющего битовую маску новых прав доступа.

Формат символьного режима:

chmod *[ugoa...][[+-=][rwxXstugo...]...][,...] имя_файла*

Каждый аргумент — это список символьных команд изменения прав доступа, разделенных запятыми. Каждая такая команда начинается с нуля или более букв *ugoa*, комбинация которых указывает, чьи права доступа к файлу будут изменены: пользователя, владеющего файлом (U); пользователей в данной группе (g); остальных пользователей, не входящих в данную группу (o), или же всех пользователей (a). Буква a эквивалентна ugo. Если не задана ни одна буква, то автоматически будет использоваться буква *a*, но биты, установленные в umask, не будут затронуты.

Оператор «+» добавляет выбранные права доступа к уже имеющимся у каждого файла; «-» удаляет эти права; а «=» присваивает только эти права каждому указанному файлу.

Буквы *rwxXstugo* выбирают новые права доступа для пользователя, заданного одной из букв *ugoa*; чтение (Г); запись (W); исполнение (или доступ к каталогу) (X); выполнение, если файл является каталогом или уже имеет право на выполнение для какого-нибудь пользователя (X); setuid- или setgid-биты (S); sticky-бит (t); установка для остальных таких же прав доступа, которые имеет пользователь, владеющий этим файлом (U); установка для остальных таких же прав доступа, которые имеет группа файла (g); установка для остальных таких же прав доступа, которые имеют остальные пользователи (не входящие в группу файла) (O).

Иллюстрация и примеры использования команды ***chmod*** приведены на рисунке 34.

Рисунок 34 - Описание команды chmod

Например, для изменения типа доступа к файлу на хранилище SAMBA на полный доступ всех пользователей и групп необходимо в консоли ввести команду:

 # *chmod 777 /srv/samba/<имя_файла>*

Разрешить чтение и запись для владельца, группы и остальных пользователей можно командой:

 # *chmod 666 /srv/samba/<имя_файла>*

3.6 Создание виртуальной машины

Перед запуском процедуры создания ВМ по регламенту необходимо создать образ диска, используя следующую команду:

$ dd if=/dev/zero of=var/lib/libvirt/images/disk.img bs=1G count=5, где

if=/dev/zero – указывает на источник копирования (специальный файл *dev/zero,* представляющий собой источник нулевых байтов);

of=var/lib/libvirt/images/disk.img – указывает на файл назначения (*disk.img* – имя создаваемого образа диска);

bs=1G – размер блока записи, который будет записан за один раз;

count=5 – количество блоков для записи.

Примечание: Дальнейшее изменение размера дискового пространства под ВМ невозможно, поэтому будьте внимательны при выделении хранилища.

Для создания виртуальной машины необходимо зайти в меню *Приложения-> Системные->Менеджер виртуальных машин*, после чего откроется окно **Менеджер виртуальных машин** (рисунок 35). В верхней части окна расположено меню для управления виртуальными машинами, в нижней части окна – список уже существующих виртуальных машин на сервере виртуализации.

Рисунок 35 – Менеджер виртуальных машин

Для того чтобы создать новую виртуальную машину, необходимо нажать кнопку **Создать новую виртуальную машину** (рисунок 35), после чего откроется окно **Новая виртуальная машина** (рисунок 36).

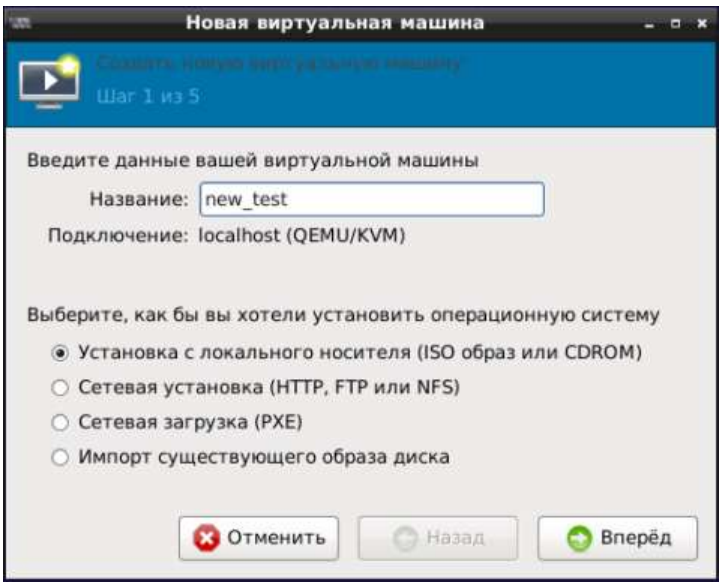


Рисунок 36 – Новая виртуальная машина. Шаг 1

Процесс создания новой ВМ состоит из нескольких шагов. На первом шаге (рисунок 36) необходимо ввести название виртуальной машины и выбрать при помощи переключателя один из способов установки операционной системы (ОС) на виртуальную машину:

- Установка с локального носителя (ISO образ или CD-ROM);
- Сетевая установка (HTTP, FTP или NFS);
- Сетевая загрузка (PXE);
- Импорт существующего образа диска.

Если была выбрана установка с локального носителя, то после заполнения всех полей и нажатия кнопки **Вперед** (рисунок 36) откроется окно со следующим шагом создания ВМ (рисунок 37).

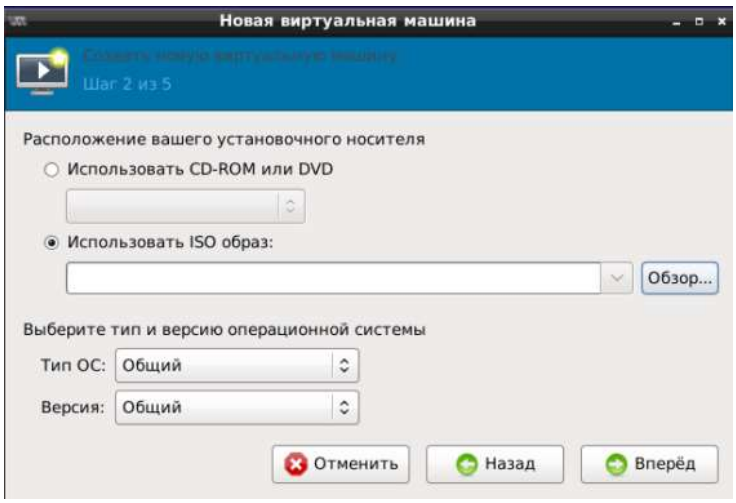


Рисунок 37 – Новая виртуальная машина. Установка с локального носителя

В данном окне при помощи переключателя необходимо указать расположение установочного носителя:

1. CD-ROM или DVD. Следует вставить носитель с записанным на него установочным файлом ОС в CD/DVD-привод сервера, “примонтировать” (командой *mount* в консоли), и затем выбрать его из раскрывающегося списка.
2. ISO образ. Если установочный носитель выполнен в виде ISO образа, следует указать путь к местонахождению файла с образом. Для этого нужно нажать кнопку **Обзор** (рисунок 37), найти в файловом менеджере файл образа и нажать кнопку **Открыть** (рисунок 38).

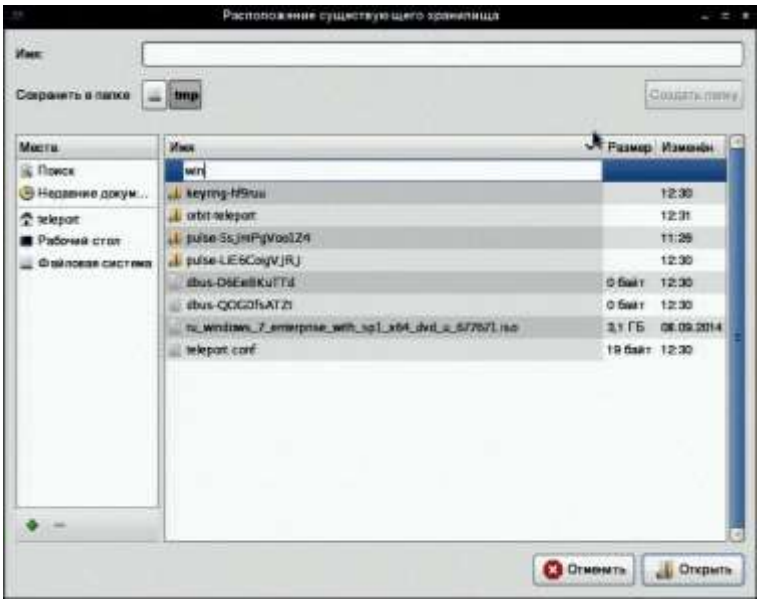


Рисунок 38 – Файловый менеджер

После указания месторасположения носителя ОС следует выбрать из раскрывающегося списка тип и версию ОС и нажать кнопку **Вперед** (рисунок 37).

Если на первом шаге (рисунок 36) была выбрана сетевая установка (HTTP, FTP или NFS), то в поле следует указать URL установки ОС. Можно выбрать тип и версию ОС из раскрывающихся ниже списков, если отключить флажок **Автоматически определять операционную систему на установочном носителе** (рисунок 39).

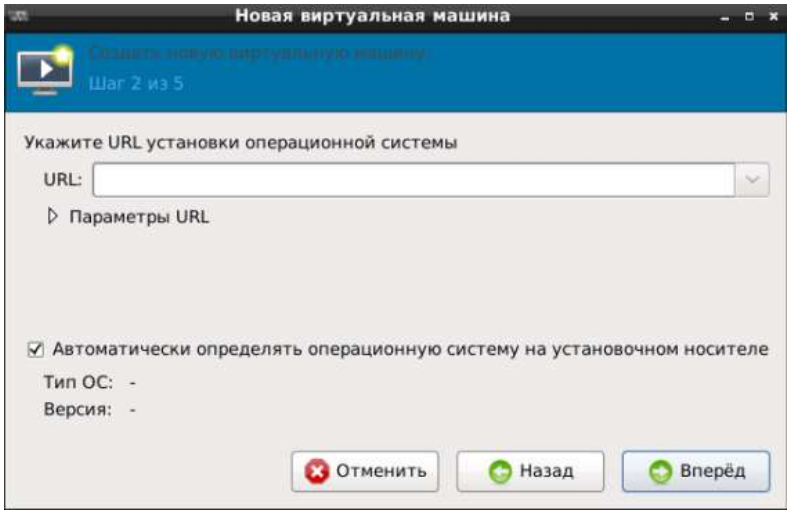


Рисунок 39 – Новая виртуальная машина. Сетевая установка

Если на первом шаге (рисунок 36) была выбрана сетевая загрузка (PXE), то следует выбрать тип и версию операционной системы из раскрывающихся ниже списков. Возможные типы операционной системы: общий тип, Linux, Other, Solaris, UNIX и Windows (рисунок 40).

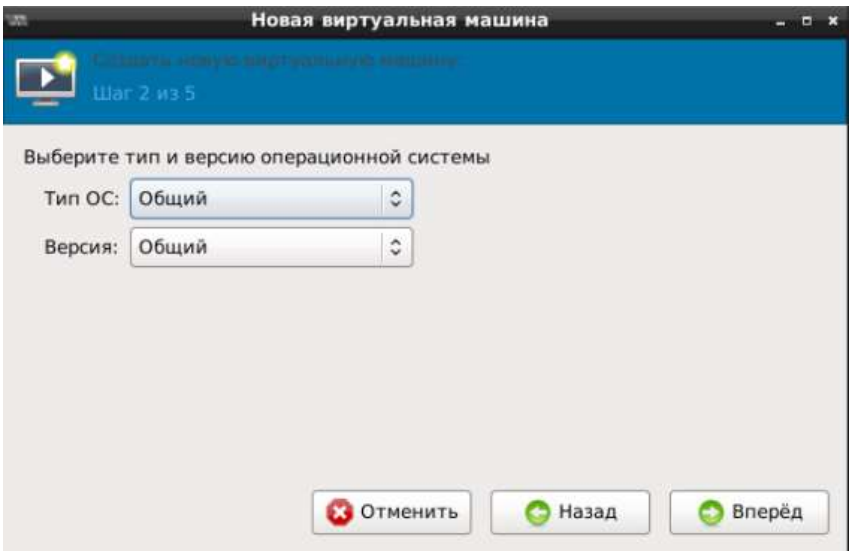


Рисунок 40 – Новая виртуальная машина. Сетевая загрузка

Если на первом шаге (рисунок 36) был выбран импорт существующего образа диска, то следует указать путь к существующему хранилищу и выбрать тип и версию операционной системы из раскрывающихся ниже списков. Возможные типы операционной системы: общий тип, Linux, Other, Solaris, UNIX и Windows (рисунок 41).

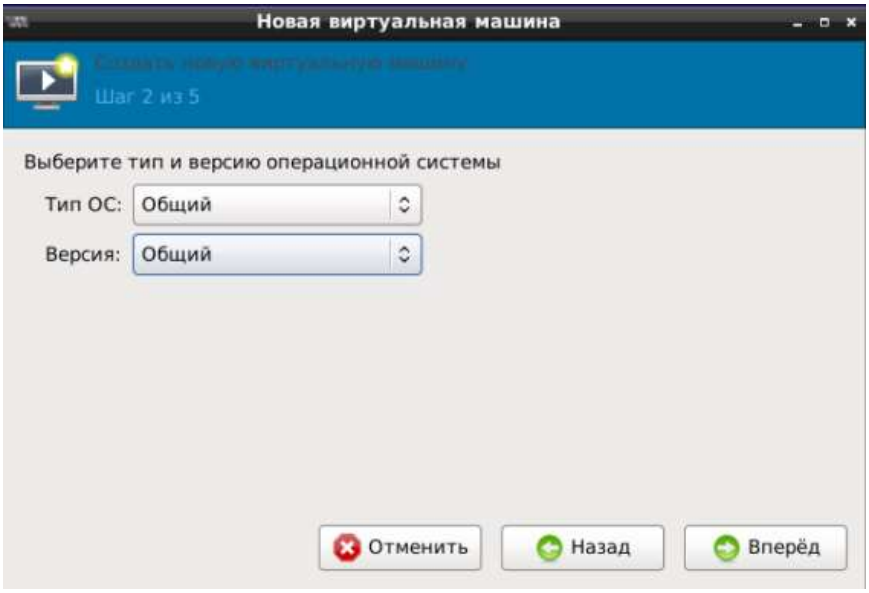


Рисунок 41 – Новая виртуальная машина. Импорт существующего образа диска

На следующем шаге необходимо указать количество оперативной памяти и число процессоров (CPU), которые будут выделены для виртуальной машины, и нажать кнопку **Вперед** (рисунок 42).

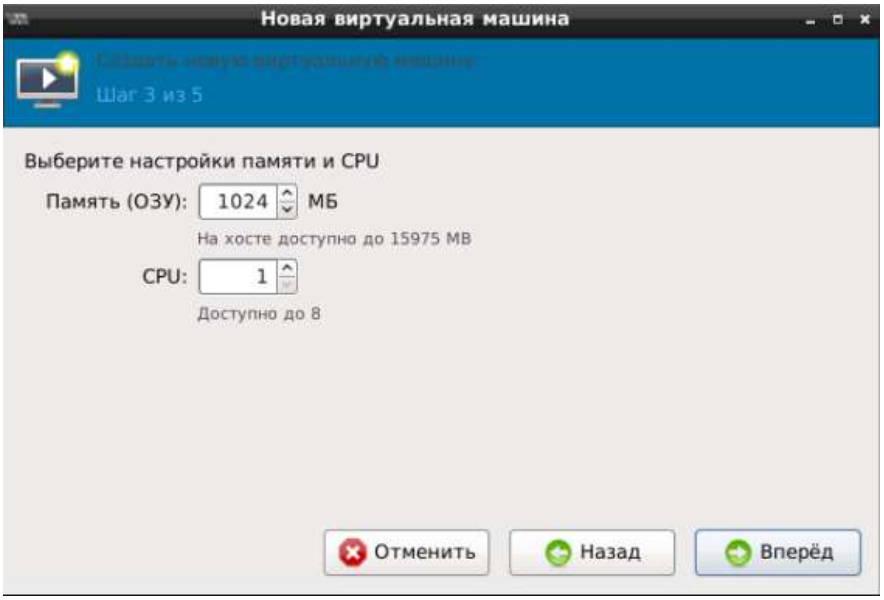


Рисунок 42 – Новая виртуальная машина. Шаг 3

Далее следует включить хранилище, установив флажок **Включить хранилище для этой виртуальной машины.** Установить переключатель в позицию **Выберите управляемое или другое существующее хранилище** (рисунок 43). При помощи кнопки **Обзор** найти в файловом менеджере созданное описанным выше способом хранилище и нажать кнопку **Открыть**.

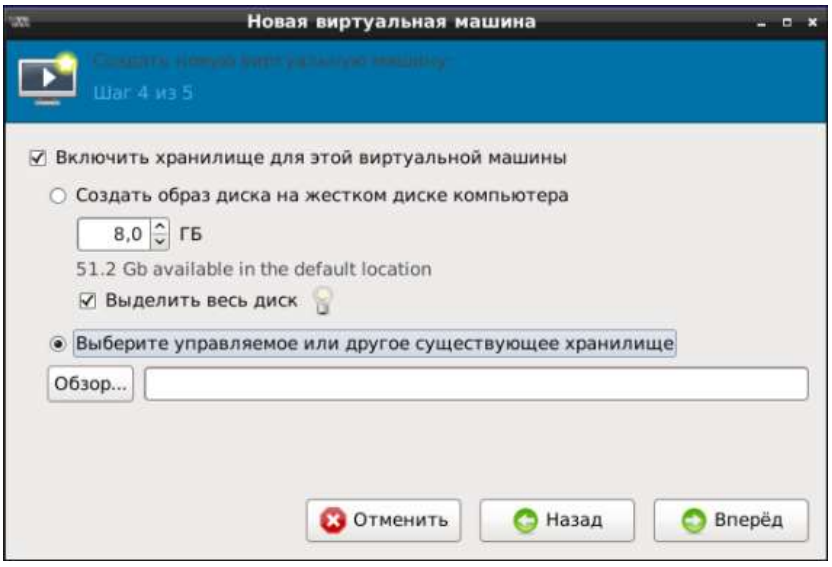


Рисунок 43 – Новая виртуальная машина. Шаг 4

На следующем шаге откроется окно для проверки выбранных настроек, в котором также можно указать дополнительные параметры ВМ (рисунок 44).

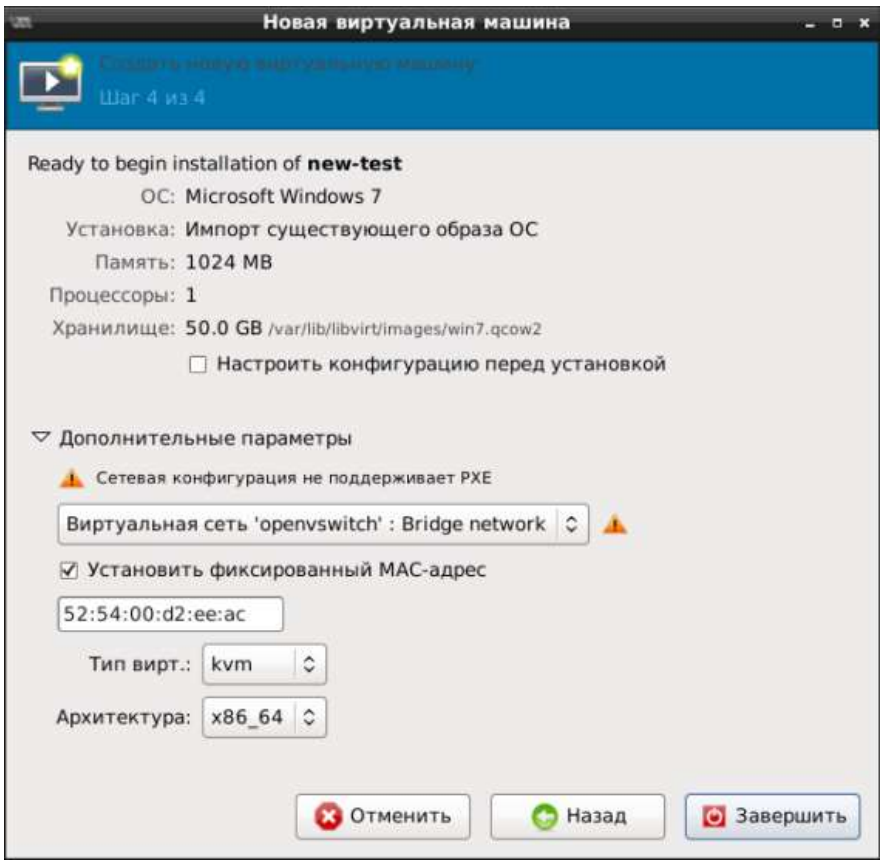


Рисунок 44 – Новая виртуальная машина. Шаг 5

Из раскрывающегося списка можно выбрать виртуальную сеть.

При необходимости можно задать фиксированный MAC-адрес устройства путем установки соответствующего флажка, тип виртуализации (kvm или qemu) и архитектуру ОС (i686 или x86_64).

Чтобы внести изменения, следует нажать кнопку **Назад**. Для начала инсталляции выбранной ОС следует нажать кнопку **Завершить**.

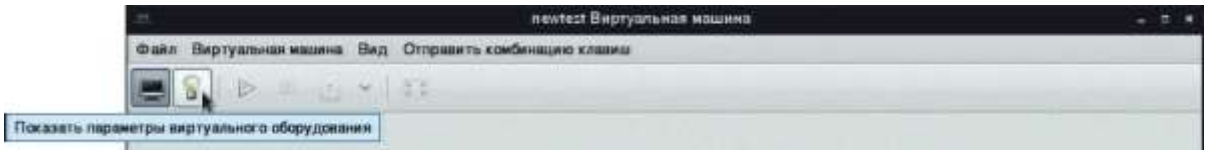
ВНИМАНИЕ. Для подключения тонкого клиента к ВМ необходим графический сервер Spice. По умолчанию в новой виртуальной машине создается графический сервер VNC, поэтому необходимо отредактировать параметры ВМ (подробнее о настройке графического сервера см. раздел 3.7.9 настоящего руководства).

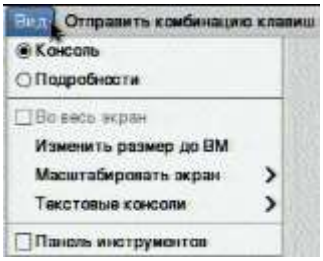
3.7 Настройка виртуальной машины

Для настройки виртуальной машины необходимо зайти в меню *Приложения-> Системные->Менеджер виртуальных машин*, после чего откроется окно **Менеджер виртуальных машин** (рисунок 35). Для отображения настроек необходимо открыть ВМ, кликнув два раза левой клавишей “мыши” по иконке виртуальной машины или нажать кнопку **Открыть** 

.

В открывшемся окне следует нажать кнопку **Показать параметры виртуального оборудования** или перейти в меню *Вид->Подробности.*





Откроется окно параметров виртуального оборудования ВМ (рисунок 45).

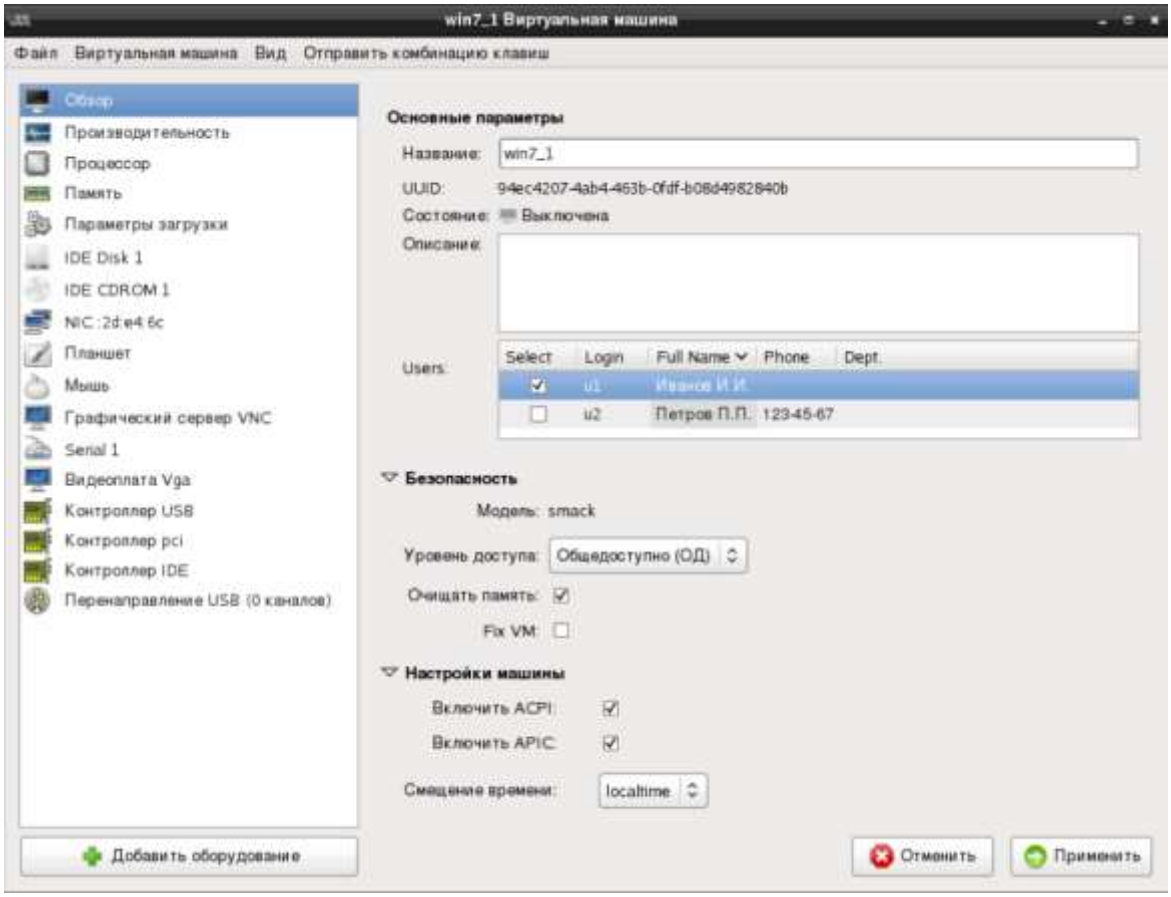


Рисунок 45 – Параметры виртуального оборудования

В левой части окна приведен список параметров и виртуальных устройств, установленных на выбранной ВМ. При выборе одного из пунктов списка, в правой части отображаются соответствующие ему настройки ВМ. Для того чтобы внесенные изменения вступили в силу, необходимо нажать кнопку **Применить**.

3.7.1 Подменю “Обзор”

Группа **Основные параметры** имеет следующие заполняемые поля:

Название – наименование виртуальной машины;

Описание – в поле можно занести дополнительную текстовую информацию о ВМ;

Users – из списка пользователей, созданных согласно п.3.4, выбирается тот, которому будет разрешен доступ к данной ВМ.

ВНИМАНИЕ. ПО РЕГЛАМЕНТУ НА ОДНУ ВМ МОЖЕТ БЫТЬ НАЗНАЧЕН ТОЛЬКО ОДИН УНИКАЛЬНЫЙ ПОЛЬЗОВАТЕЛЬ.

Группа **Безопасность** имеет следующие поля:

Уровень доступа – из раскрывающегося списка нужно выбрать один из уровней мандатного доступа. Создание мандатных категорий приведено в п. 3.5.1.

Очищать память – при установленном флажке будет принудительно очищаться оперативная память.

ВНИМАНИЕ. С ЦЕЛЬЮ РЕАЛИЗАЦИИ ТРЕБОВАНИЙ ЗАЩИТЫ ОТ НСД В ЧАСТИ ОЧИСТКИ ПАМЯТИ ФЛАЖОК **ОЧИЩАТЬ ПАМЯТЬ** ДОЛЖЕН БЫТЬ УСТАНОВЛЕН ОБЯЗАТЕЛЬНО.

Fix VM – флажок может быть установлен администратором для того, чтобы при дальнейшей работе ВМ каждый раз восстанавливалась из первоначального состояния.

ВНИМАНИЕ. ПРИ НЕОБХОДИМОСТИ ВНЕСТИ ИЗМЕНЕНИЯ В КОНФИГУРАЦИЮ ВМ ИЛИ УСТАНОВИТЬ ПО В СРЕДУ ГОСТЕВОЙ ОС СЛЕДУЕТ СНЯТЬ ФЛАЖОК **FIX VM**, НАЖАТЬ КНОПКУ **ПРИМЕНИТЬ**, ВНЕСТИ НЕОБХОДИМЫЕ ИЗМЕНЕНИЯ И ВНОВЬ УСТАНОВИТЬ ФЛАЖОК **FIX VM**.

Группа **Настройки машины** имеет следующие поля:

Включить ACPI – при установленном флажке гостевой системе могут предоставляться функции интерфейса управления питанием;

Включить APIC – при установленном флажке будет включен улучшенный контроллер прерываний ввода/вывода (APIC).

3.7.2 Подменю “Производительность”

В подменю “Производительность” (рисунок 46) выводятся статистические данные об использовании памяти, загрузке процессора, дисковых и сетевых вводах/выводах.

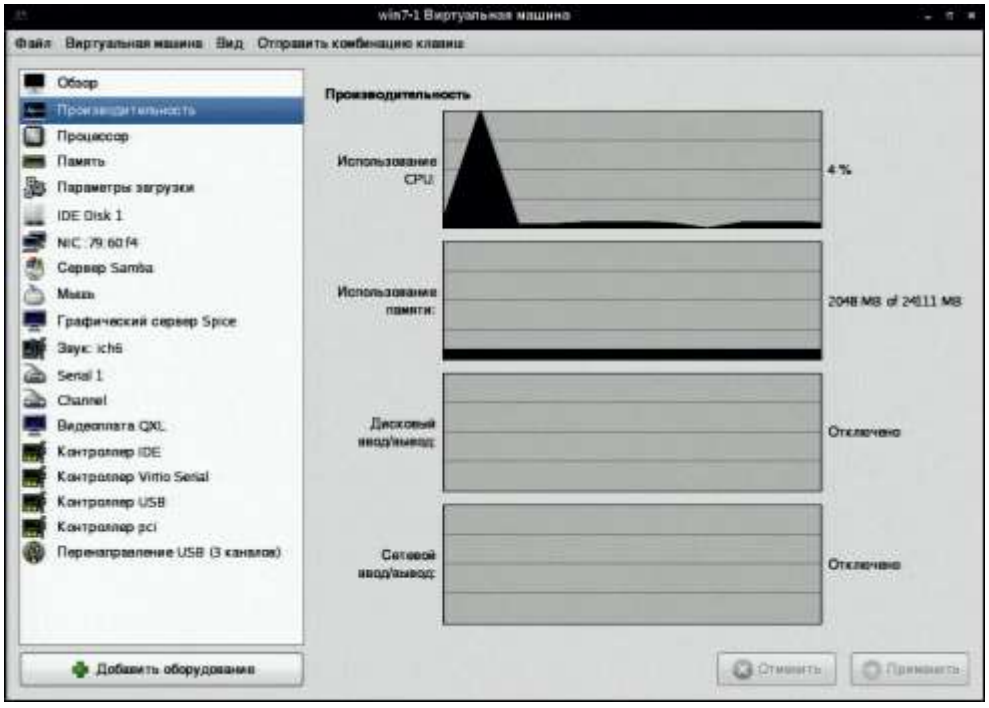


Рисунок 46 – Подменю «Производительность»

3.7.3 Подменю “Процессор”

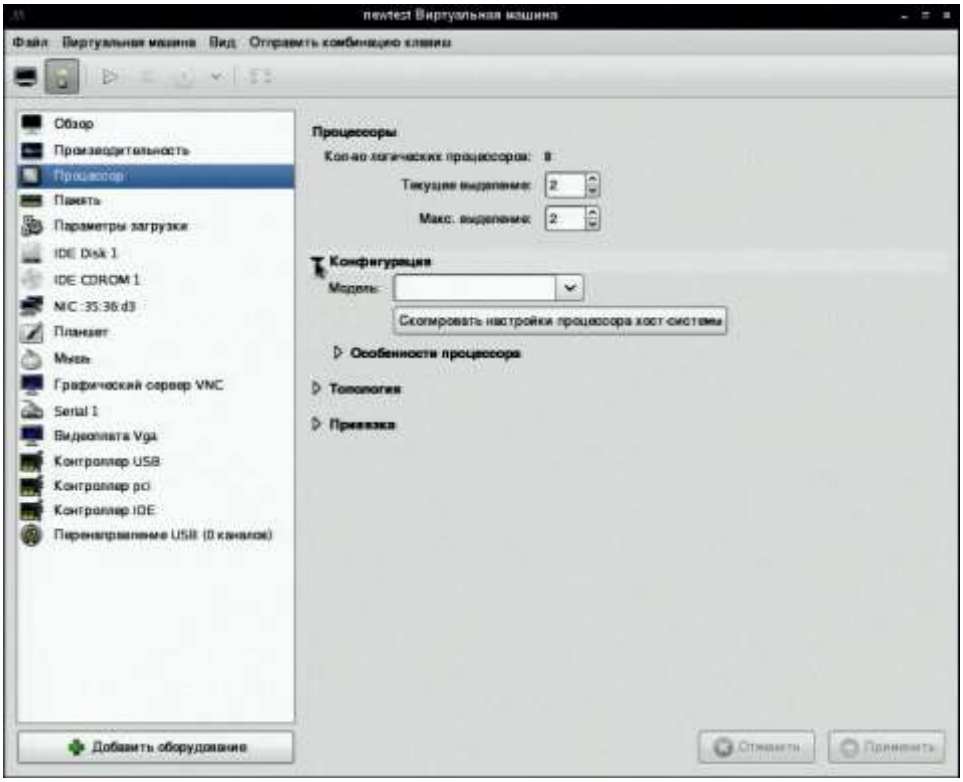


Рисунок 47 – Подменю «Процессор»

В группе полей **Процессоры** необходимо указать текущее и максимально возможное количество процессоров, выделяемых для ВМ.

3.7.4 Подменю “Память”

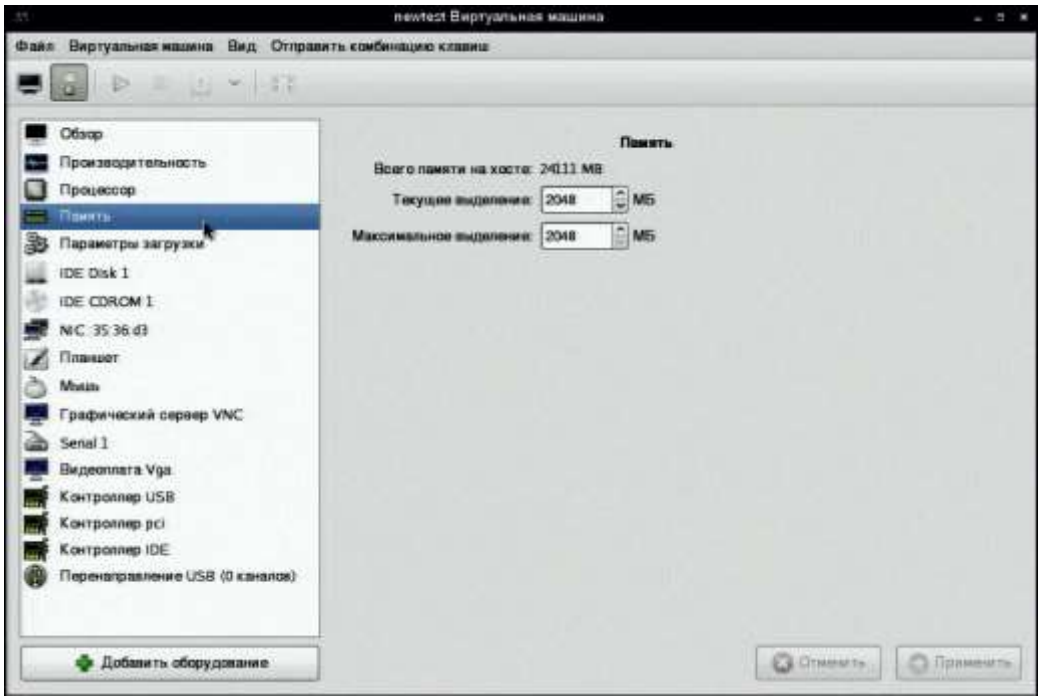


Рисунок 48 – Подменю «Память»

В данном подменю задается объем выделяемой оперативной памяти для ВМ.

3.7.5 Подменю “Параметры загрузки”

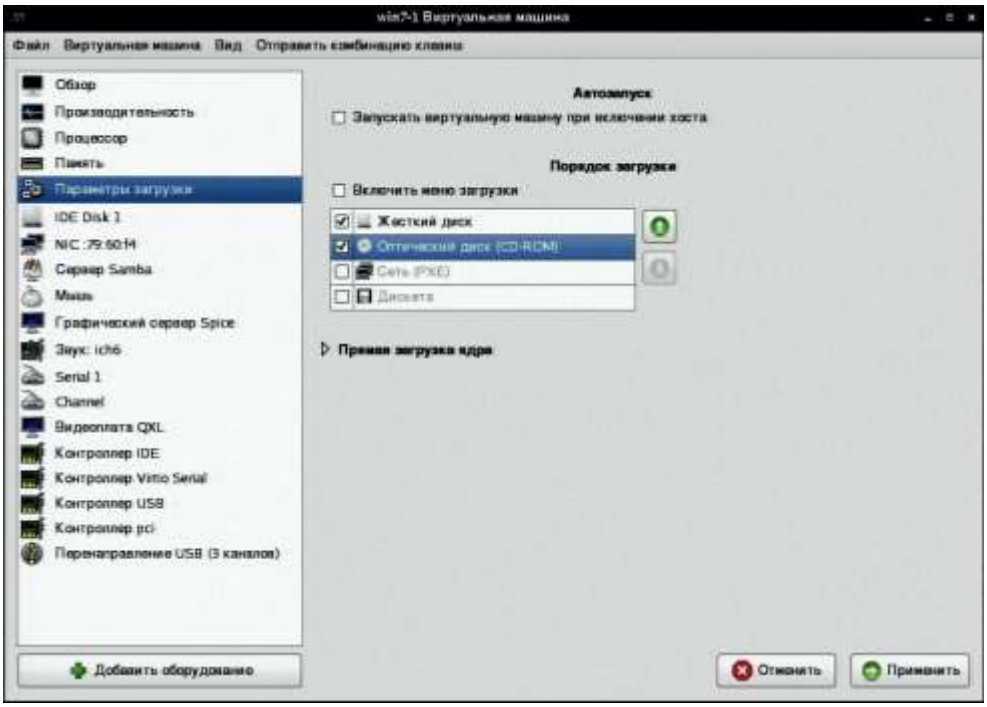


Рисунок 49 – Подменю «Параметры загрузки»

В подменю “Параметры загрузки” можно установить флажок о необходимости запуска виртуальной машины при включении сервера виртуализации.

Также можно определить порядок устройств, в котором ВМ будет пытаться загрузить гостевую ОС. Если установлен флажок **Включить меню загрузки**, то становится активной таблица устройств. ВМ может указать для гостевой ОС, что необходимо загрузиться с жесткого диска, оптического диска (CD-ROM), дискеты или сети (PXE). По умолчанию система загружается с жесткого диска. Для того чтобы изменить порядок загрузки, следует выделить строку с названием устройства и при помощи стрелок справа от таблицы переместить ее на желаемую позицию.

3.7.6 Подменю “IDE Disk 1”

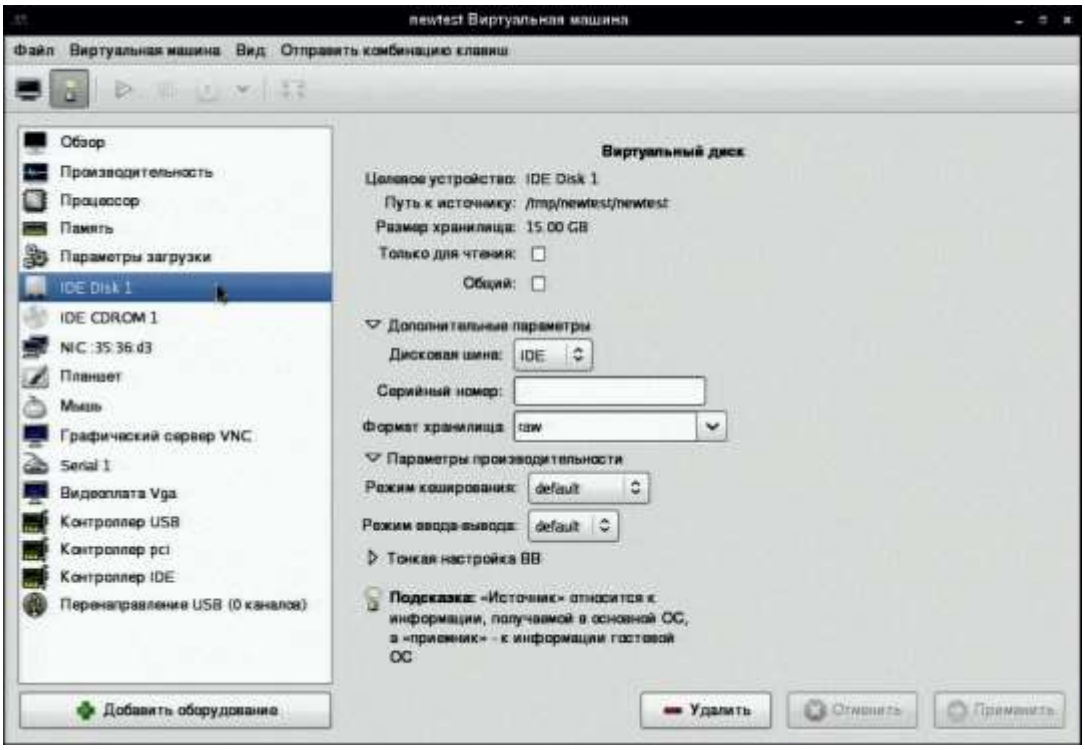


Рисунок 50 – Подменю “IDE Disk 1”

В данном подменю производится настройка виртуального жесткого диска.

В окне на рисунке 50 приводится название целевого устройства, путь к виртуальному жесткому диску на сервере и размер хранилища.

При установке флажка **Только для чтения**, информацию, хранящуюся на виртуальном диске невозможно будет изменить.

3.7.7 Подменю “NIC :35:36:d3”

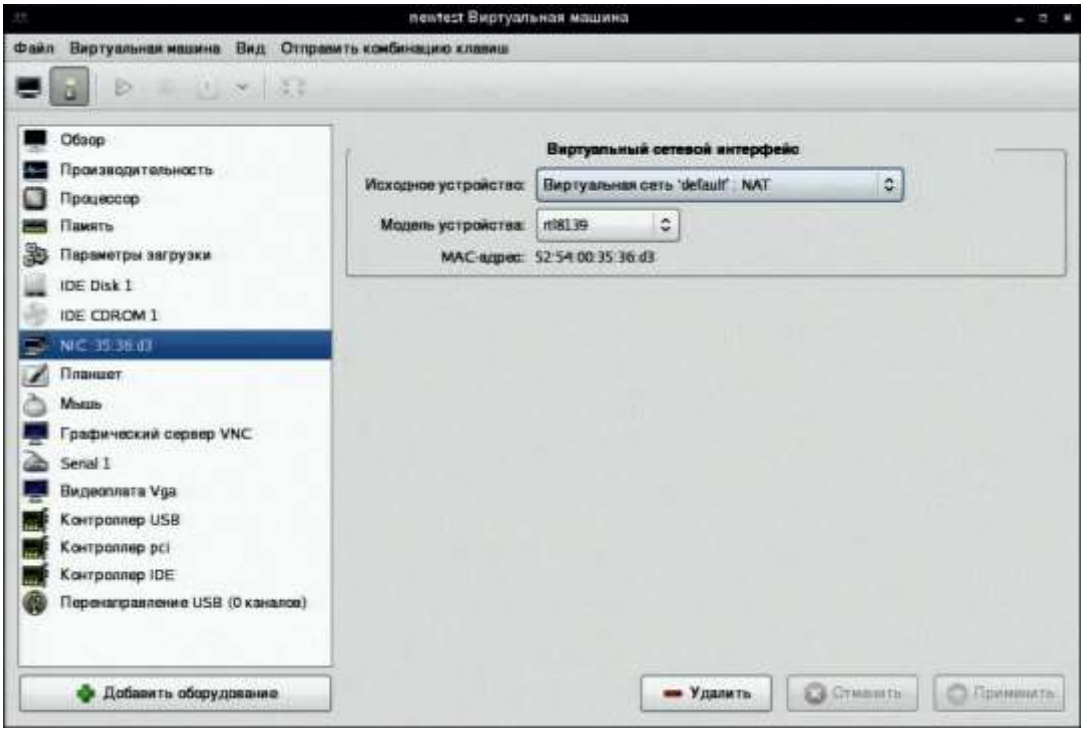


Рисунок 51 – Подменю “NIC :35:36:d3”

В данном подменю указывается выбор физического или виртуального сетевого интерфейса для подключения виртуальной сетевой карты и её модель.

3.7.8 Подменю “Планшет” и “Мышь”

Данные подменю необходимы для корректной работы с ВМ, при подключении TouchPad, сенсорного экрана либо “мыши”.

3.7.9 Подменю “Графический сервер”

Для подключения *терминалов* к виртуальной машине используется графический сервер Spice. Перед этим необходимо удалить созданный по умолчанию графический сервер VNC, для чего следует выделить его в списке устройств и нажать кнопку **Удалить**.

Для создания графического сервера Spice нужно нажать кнопку **Добавить оборудование** (рисунок 45), в открывшемся окне **Добавить новое виртуальное устройство** (рисунок 52) в списке устройств слева выбрать пункт **Графика**. В поле **Тип** следует указать значение ***Сервер spice***, обязательно установить флажок **Прослушивать все общедоступные интерфейсы** и нажать кнопку **Завершить**.

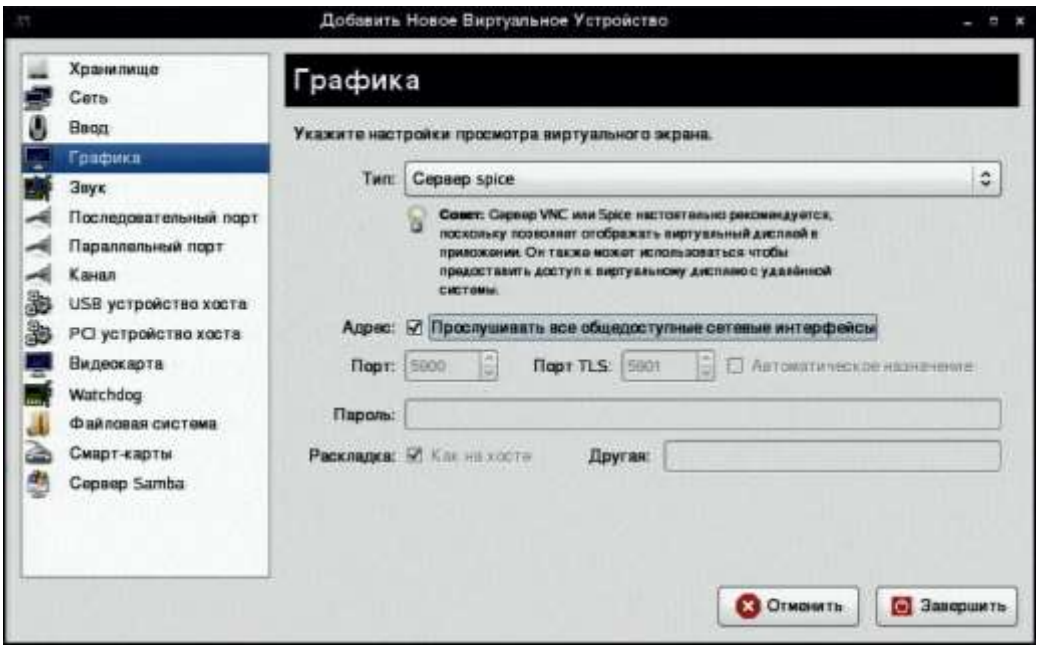


Рисунок 52 – Добавление графического сервера

После этого в списке устройств появится Графический сервер Spice (рисунок 53).

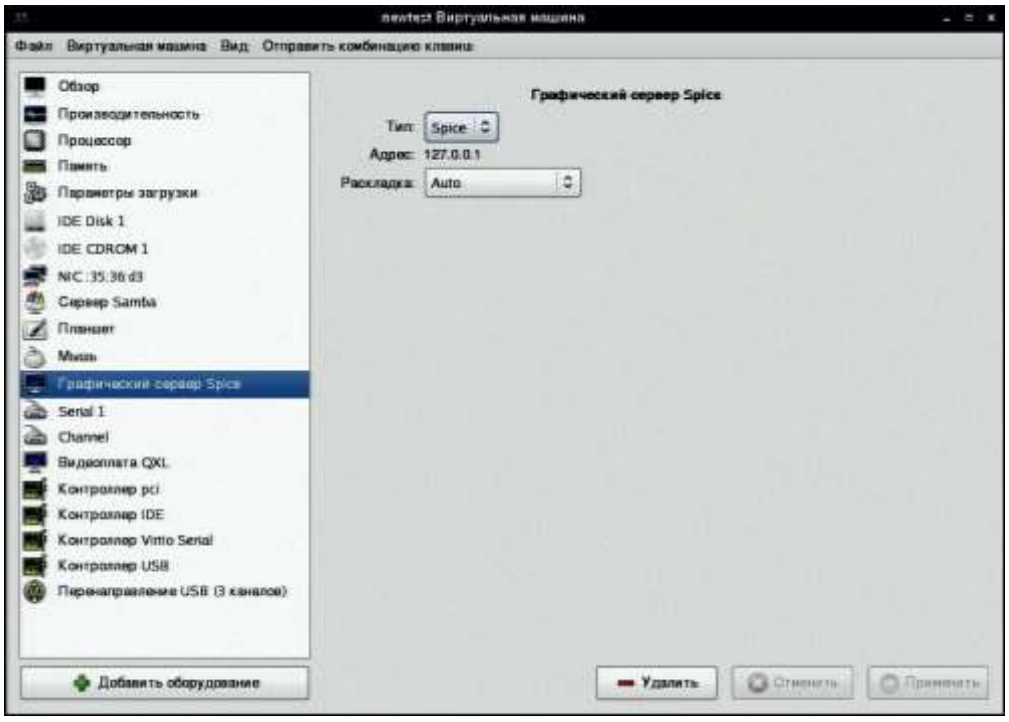


Рисунок 53 – Подменю «Графический сервер»

3.7.10 Подменю “Видеоплата”

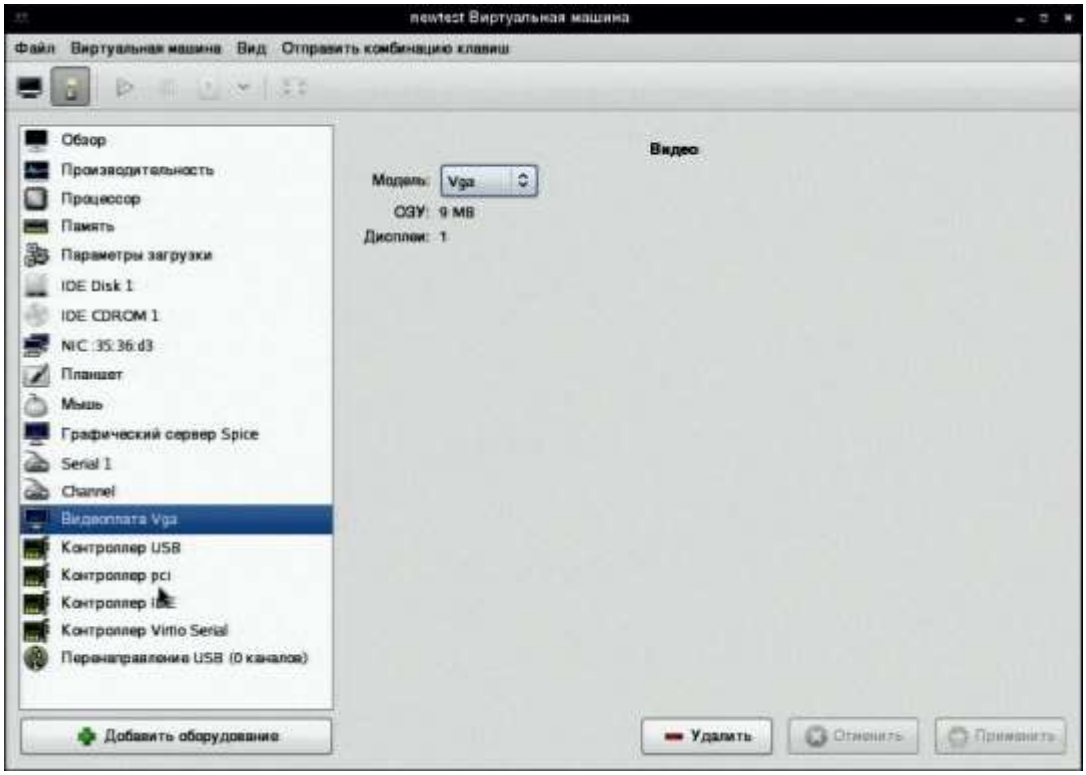


Рисунок 54 – Подменю “Видеоплата”

В подменю “**Видеоплата**” необходимо из раскрывающегося списка выбрать подходящую[1] для типа ОС ВМ модель видеоинтерфейса. Для нее указывается размер памяти, предоставляемой виртуальной графической карте и количество дисплеев.

3.7.11 Подменю “Перенаправление устройств USB”

В данном подменю регистрируются USB-устройства, которые будут подключаться к терминалу.

ВНИМАНИЕ. Незарегистрированные на *сервере виртуализации* USB-устройства на *терминале* работать не будут.

[1] Подробную информацию о соответствии модели видеоплаты и ОС можно уточнить у производителя ОС.

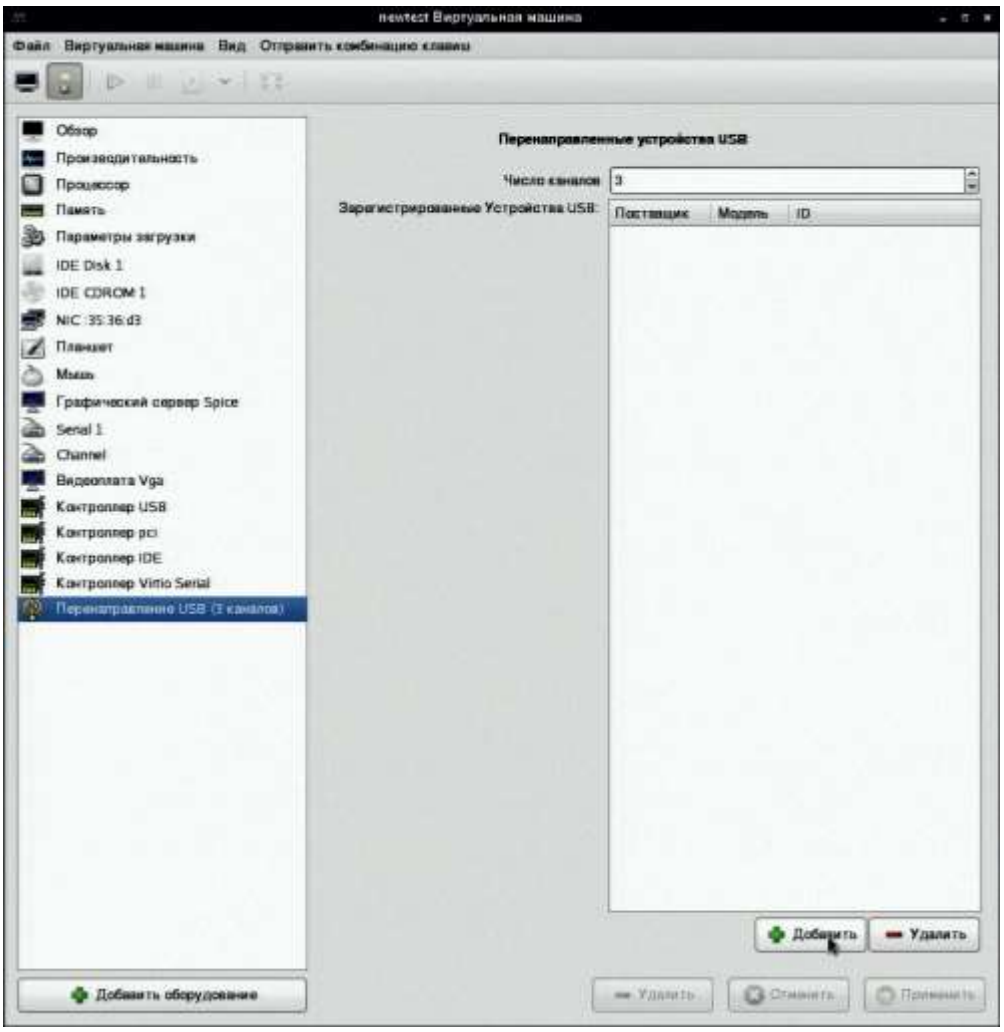


Рисунок 55 – Подменю «Перенаправление устройств USB»

В поле **Число каналов** необходимо указать, сколько USB-устройств можно будет использовать одновременно на терминале.

Регистрация новых устройств состоит из нескольких последовательных шагов:

1. В окне на рисунке 55 следует нажать кнопку **Добавить**.
2. После появления окна с требованием вставить устройство USB для регистрации (рисунок 56) вставить USB-накопитель в свободный USB-разъем сервера виртуализации.

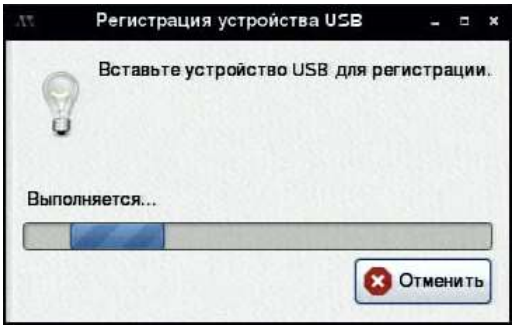


Рисунок 56 – Регистрация устройств USB

3. Дождаться, когда в списке зарегистрированных устройств появится новая строка с указанием поставщика устройства, модели и уникального ID (рисунок 57).

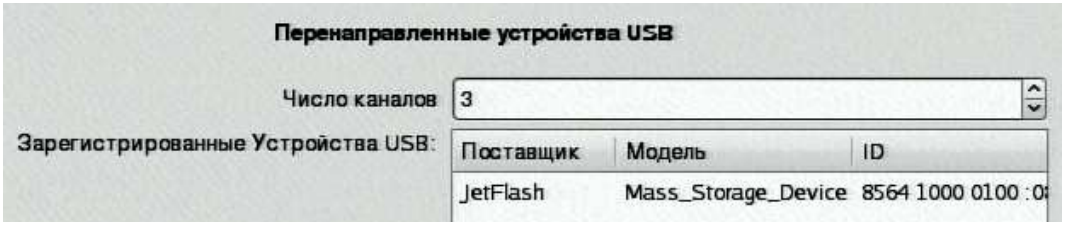


Рисунок 57 – Регистрация устройств USB

4. Извлечь зарегистрированное устройство.
5. Вставить новое устройство и повторить пункты регистрации 3,4.

После регистрации необходимого количества USB-устройств следует в окне на рисунке 56 нажать кнопку **Отменить** и в окне подменю **«Перенаправление устройств USB»** (рисунок 55) нажать кнопку **Применить**.

После регистрации всех USB-устройств в консоли необходимо перезапустить сервис vmacd командой в консоли: **service vmacd restart**.

3.8 Запуск, остановка и удаление виртуальной машины

Для запуска ВМ нужно нажать кнопку **Включить виртуальную машину** в окне **Менеджер виртуальных машин** (рисунок 35), для отключения ВМ – кнопку **Выключить виртуальную машину** (рисунок 58).

Рисунок 58 – Включение/выключение ВМ

Для того чтобы приостановить работу ВМ, следует нажать кнопку **Приостановить виртуальную машину** (рисунок 59).

Рисунок 59 – Приостановить ВМ

Также для управления состоянием ВМ предназначено раскрывающееся меню (рисунок 60). Пункт **Сохранить** нужен для создания “снимка” работающей виртуальной машины.

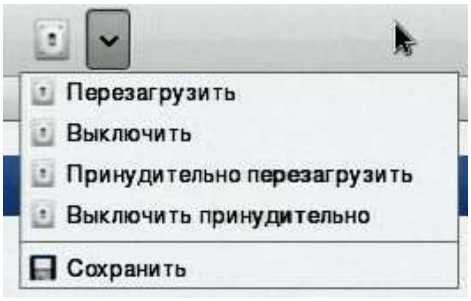


Рисунок 60 – Меню управления ВМ

Для удаления ВМ следует в **Менеджере виртуальных машин** (рисунок 35) выбрать нужную ВМ, нажать на нее правой клавишей “мыши” и выбрать пункт меню *Удалить* (рисунок 61).

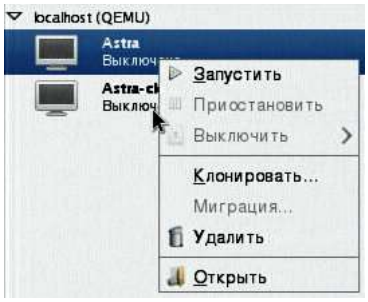


Рисунок 61 – Удаление ВМ

3.9 Настройка виртуальных сетей

Для настройки виртуальных сетей необходимо зайти в меню *Приложения-> Системные->Менеджер виртуальных машин*, после чего в **Менеджере виртуальных машин** (рисунок 62) следует выбрать пункт меню *Правка->Свойства подключения.*

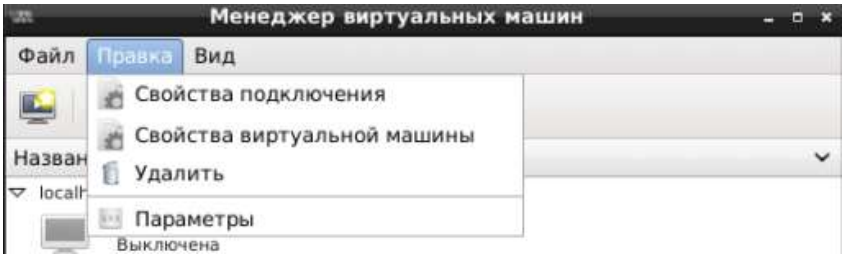


Рисунок 62 – Менеджер виртуальных машин

Откроется окно **Свойства соединения** (рисунок 63), в котором нужно выбрать вкладку **Виртуальные сети**.

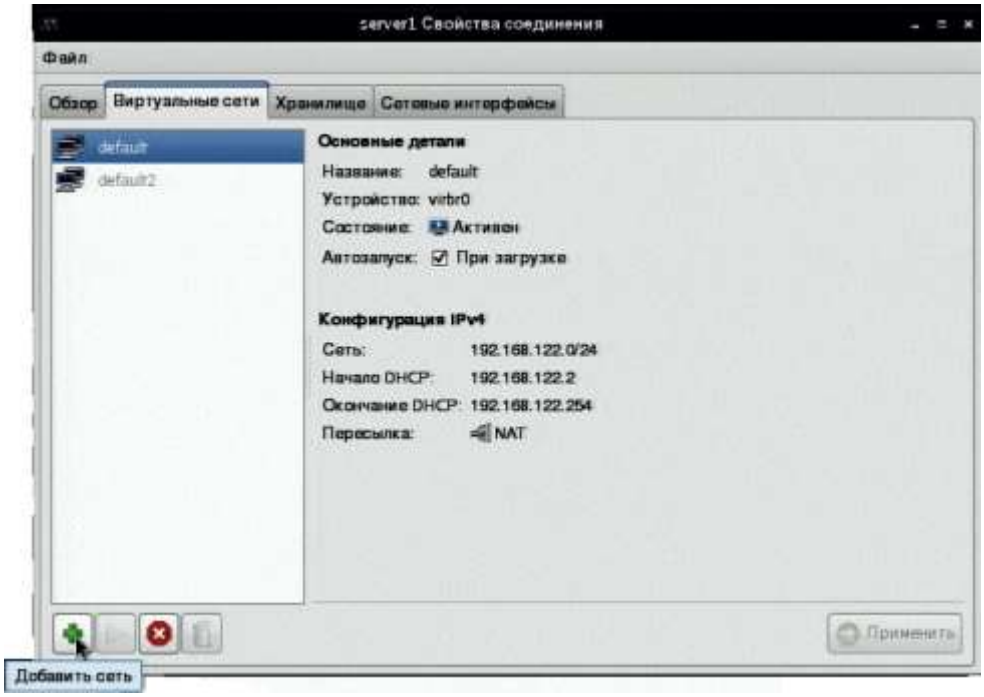


Рисунок 63 – Свойства соединения

В левой части окна приведен список виртуальных сетей, в правой – свойства выбранной сети.

Для того чтобы создать новую виртуальную сеть, нужно нажать кнопку **Добавить сеть** в левой нижней части окна, после чего запустится процесс создания сети, состоящий из нескольких шагов:

1. В первом окне помощника создания новой виртуальной сети нужно нажать кнопку **Вперед** (рисунок 64).

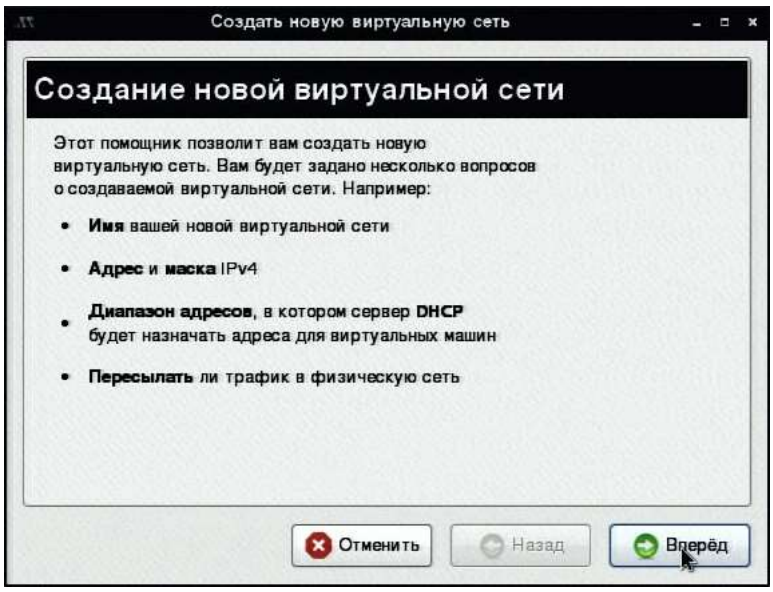


Рисунок 64 – Создание новой виртуальной сети

2. Далее следует ввести название виртуальной сети (рисунок 65).

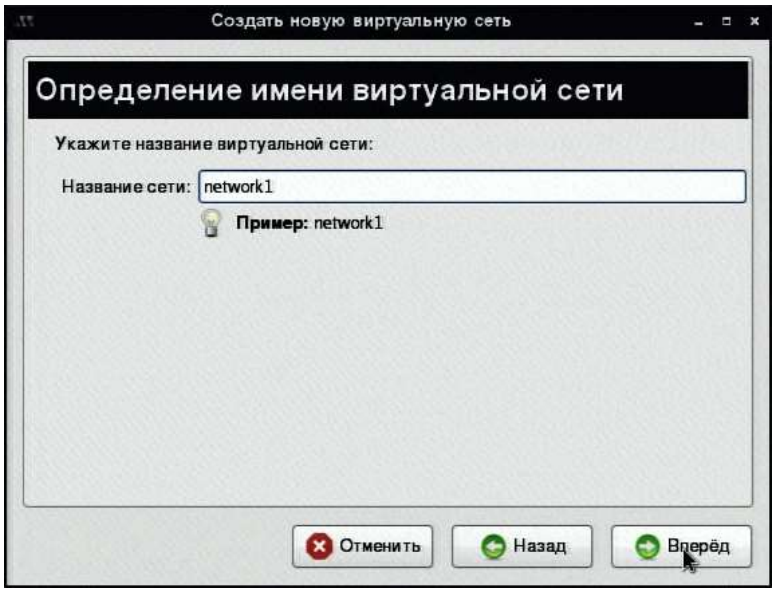


Рисунок 65 – Определение имени виртуальной сети

3. На следующем шаге нужно ввести адресное пространство Ipv4 для виртуальной сети (рисунок 66).

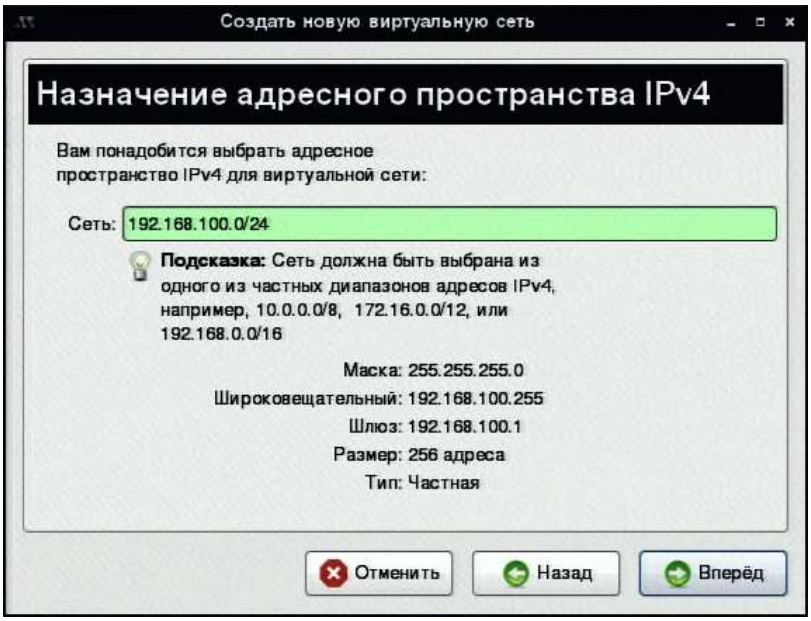


Рисунок 66 – Назначение адресного пространства Ipv4

4. Далее нужно указать диапазон адресов, которые DHCP сервер может назначить виртуальным машинам, подключенным к виртуальной сети (рисунок 67).

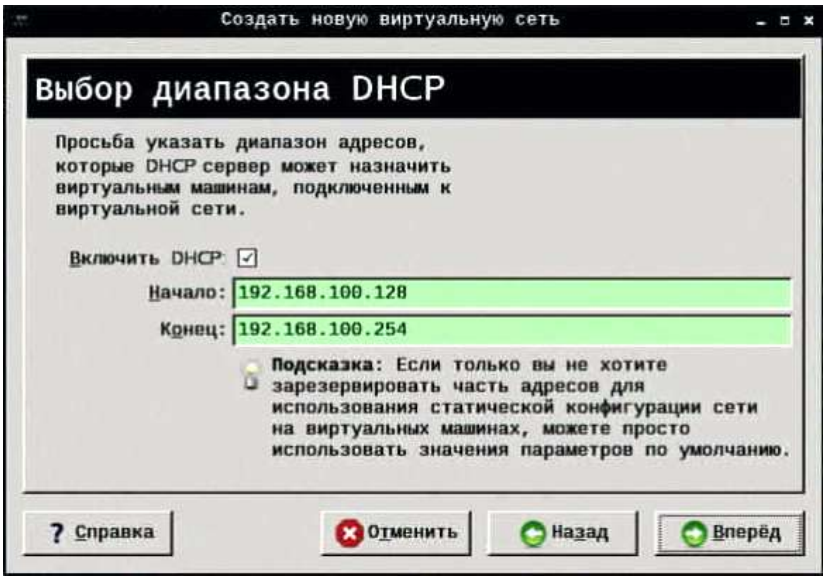


Рисунок 67 – Выбор диапазона DHCP

5. На следующем шаге нужно выбрать, является виртуальная сеть изолированной или может пересылать данные на физическое сетевое устройство (рисунок 68). При выборе второго варианта, становятся доступными выпадающие меню, в которых можно указать назначение (любое физическое устройство, физическое устройство gre0, физическое устройство lo, физическое устройство tunl0, физическое устройство vnet0, физическое устройство gretap0, физическое устройство eth0, физическое устройство eth1) и режим: NAT (трансляция адресов сети) или маршрутизирование.

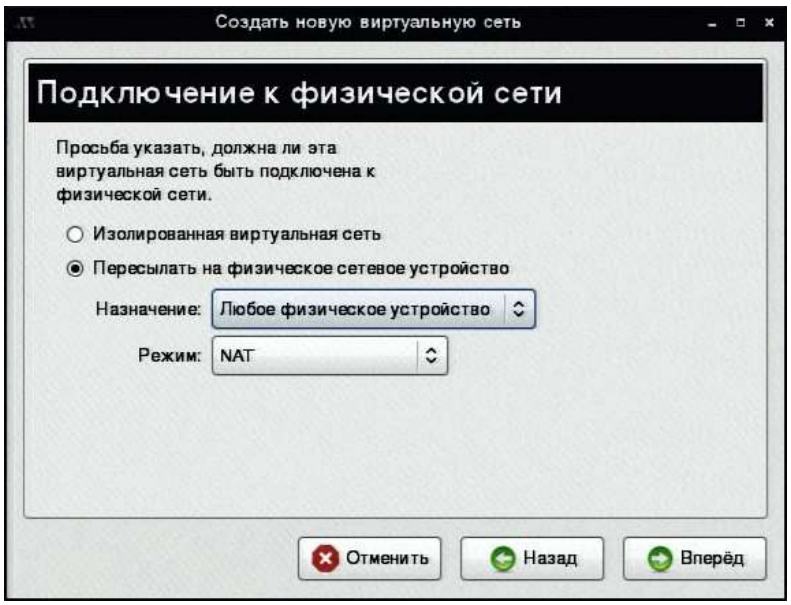


Рисунок 68 – Подключение к физической сети

6. В последнем окне выводятся введенные настройки (рисунок 69). Если все данные введены верно, нужно нажать кнопку **Завершить**. При помощи кнопки **Назад** можно вернуться к предыдущим шагам.

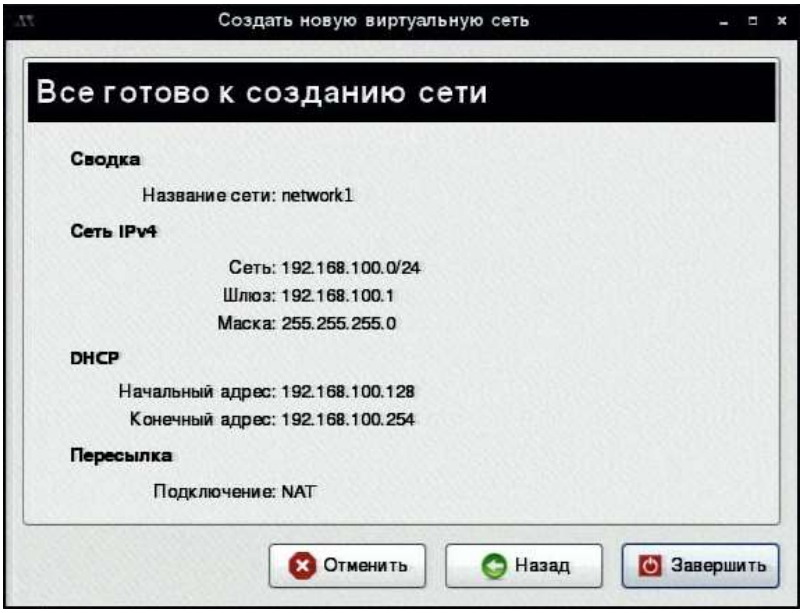


Рисунок 69 – Проверка введенных данных

В окне **Свойства соединения** (рисунок 63) появится новая сеть. При необходимости можно установить флажок **Автозапуск** для выбранной сети. После завершения всех настроек нужно нажать последовательно кнопки **Запустить сеть** и **Применить**.

3.10 Настройка виртуального коммутатора

Настройка виртуального коммутатора Open vSwitch состоит из следующей последовательности шагов:

1. Посмотреть список физических интерфейсов на сервере командой

 # ifconfig –a

Результатом будет перечень сетевых интерфейсов, в котором название физического интерфейса начинается с eth (рисунок 70).

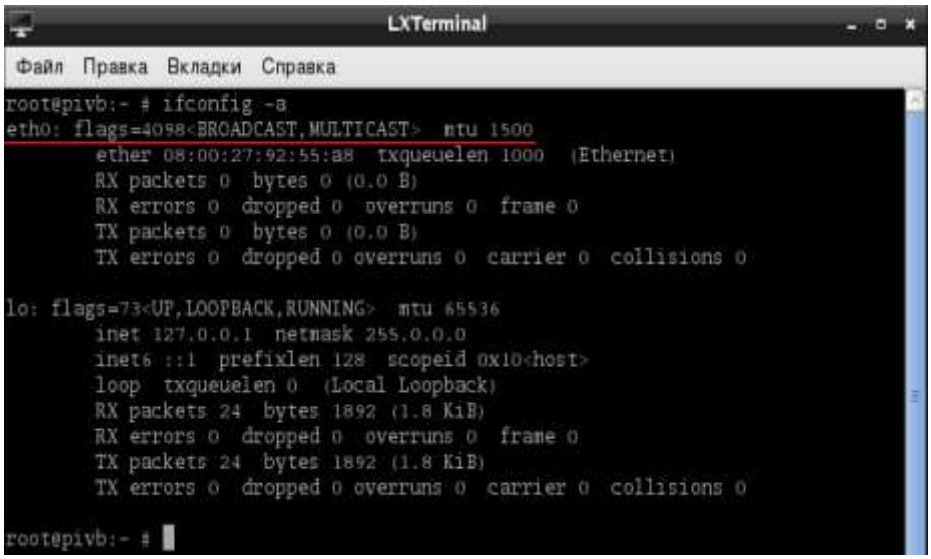


Рисунок 70

2. Перейти в директорию /network-scripts командой:

 # cd /etc/sysconfig/network-scripts

3. Для конфигурации порта физического интерфейса eth0 и внутреннего порта sys0 скопировать файл **ifcfg-lo** следующими командами:

 # cp ifcfg-lo ifcfg-eth0

 # cp ifcfg-lo ifcfg-sys0

4. Открыть для редактирования файл **ifcfg-eth0** командой:

 # mcedit ifcfg-eth0

и привести файл к следующему виду (рисунок 71):

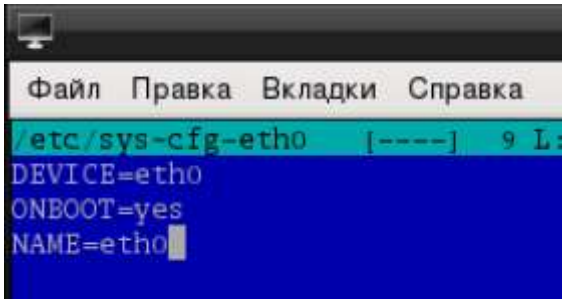


Рисунок 71

5. Открыть для редактирования файл **ifcfg-sys0** командой:

 # mcedit ifcfg-sys0

и привести файл к следующему виду (рисунок 72):

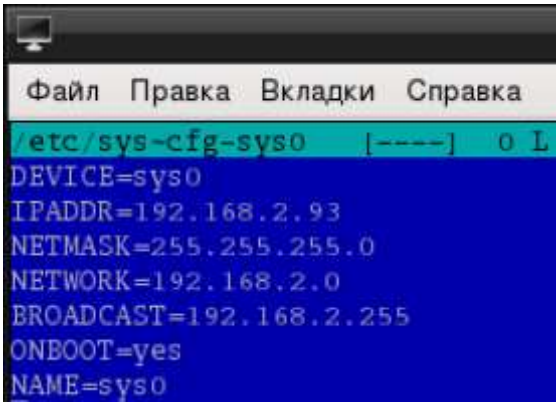


Рисунок 72

6. Создать виртуальный коммутатор Open vSwitch командой:

 # ovs-vsctl add-br hvssw0

7. Добавить к коммутатору порт физического интерфейса eth0 и внутренний порт sys0 командами:

 # ovs-vsctl add-port hvssw0 eth0

 # ovs-vsctl add-port hvssw0 sys0 – set interface sys0 type=internal

8. Перезапустить сетевые утилиты командой

 # service network restart

Также следует на всех серверах виртуализации в файл ***/etc/hosts*** следует внести информацию об именах серверов, добавив в конец строки вида:

<ip-адрес сервера виртуализации> <DNS имя сервера>

<ip-адрес сервера виртуализации> <DNS имя сервера>

3.11 Настройка сервера печати

Для настройки сервера печати необходимо зайти в меню *Приложения-> Параметры->Принтеры*, после чего откроется окно менеджера принтеров (рисунок 73).

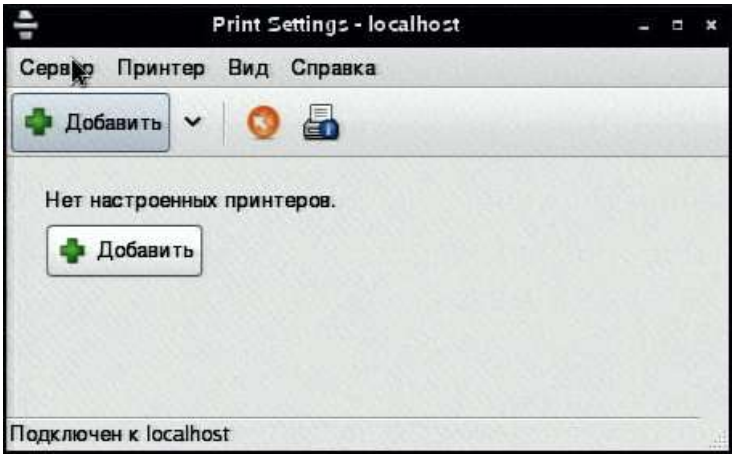


Рисунок 73 – Менеджер принтеров

3.11.1 Добавление нового принтера

Для того чтобы добавить новый принтер, следует нажать кнопку **Добавить** (рисунок 73) – откроется окно **Новый принтер** (рисунок 74).

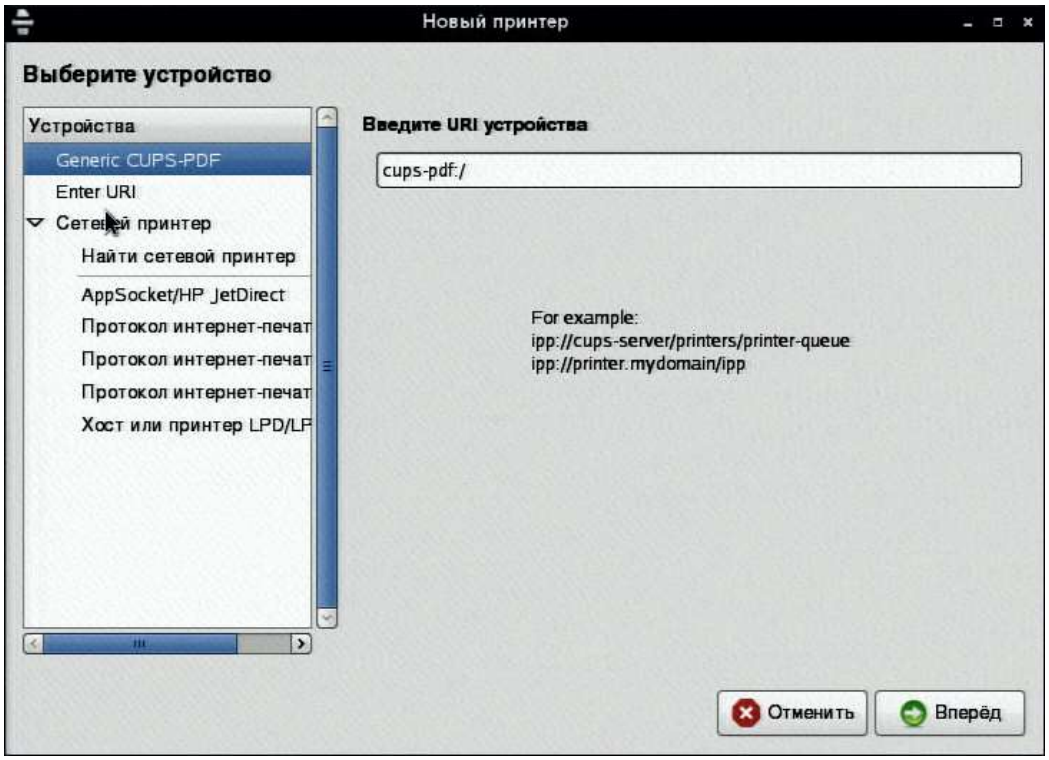


Рисунок 74 – Окно «Новый принтер»

В левой части окна приведен список устройств, которые можно подключить к серверу, в правой – поле ввода URI для доступа к выбранному устройству. После заполнения всех полей следует нажать кнопку **Вперед** – откроется окно для выбора драйвера принтера (рисунок 75).

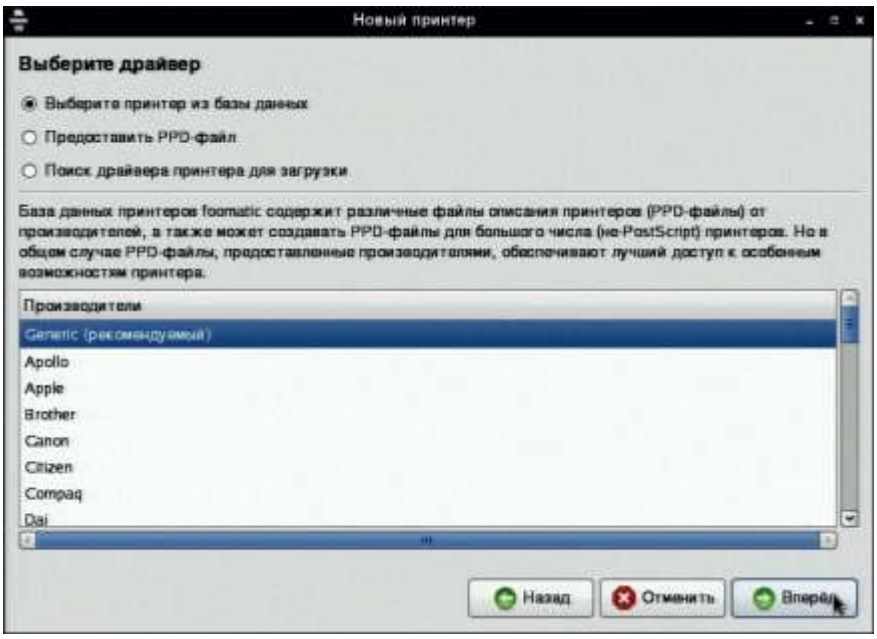


Рисунок 75 – Окно для выбора драйвера

В верхней части окна при помощи переключателя нужно выбрать место, откуда будет загружен драйвер принтера.

Если переключатель установлен в положение “**Выберите принтер из базы данных**”, то в нижней части окна (рисунок 75) следует выбрать из предложенного списка производителя принтера.

Если переключатель установлен в положение “**Предоставить PPD-файл**”, то в нижней части окна (рисунок 76) следует нажать на иконку  и в файловом менеджере найти нужный файл драйвера.

Рисунок 76 – Предоставление PPD-файла

Если переключатель установлен в положение “**Поиск драйвера принтера для загрузки**”, то в нижней части окна (рисунок 77) следует ввести марку и модель принтера и нажать кнопку **Поиск**.

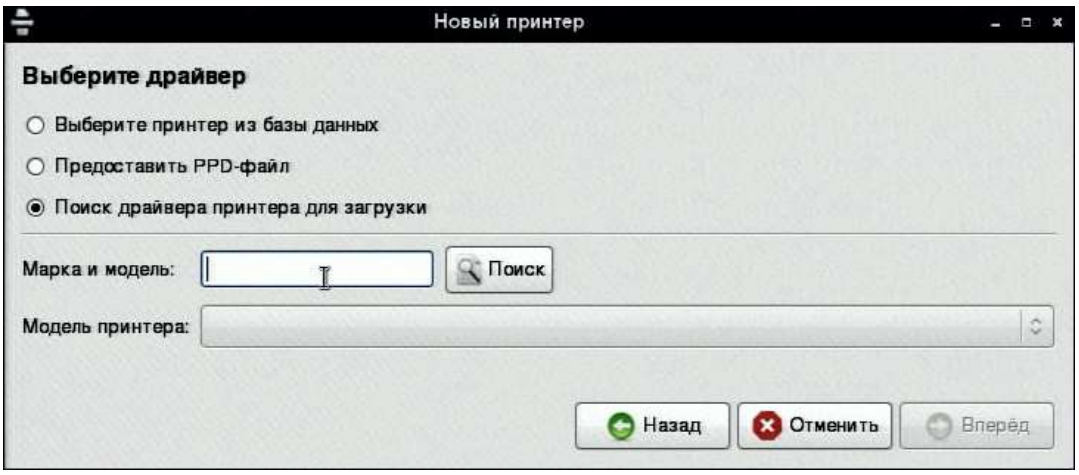


Рисунок 77 – Поиск драйвера принтера для загрузки

После выбора драйвера принтера следует нажать кнопку **Вперед** – откроется окно, в котором необходимо сопоставить выбранный принтер и драйвер (рисунок 78).

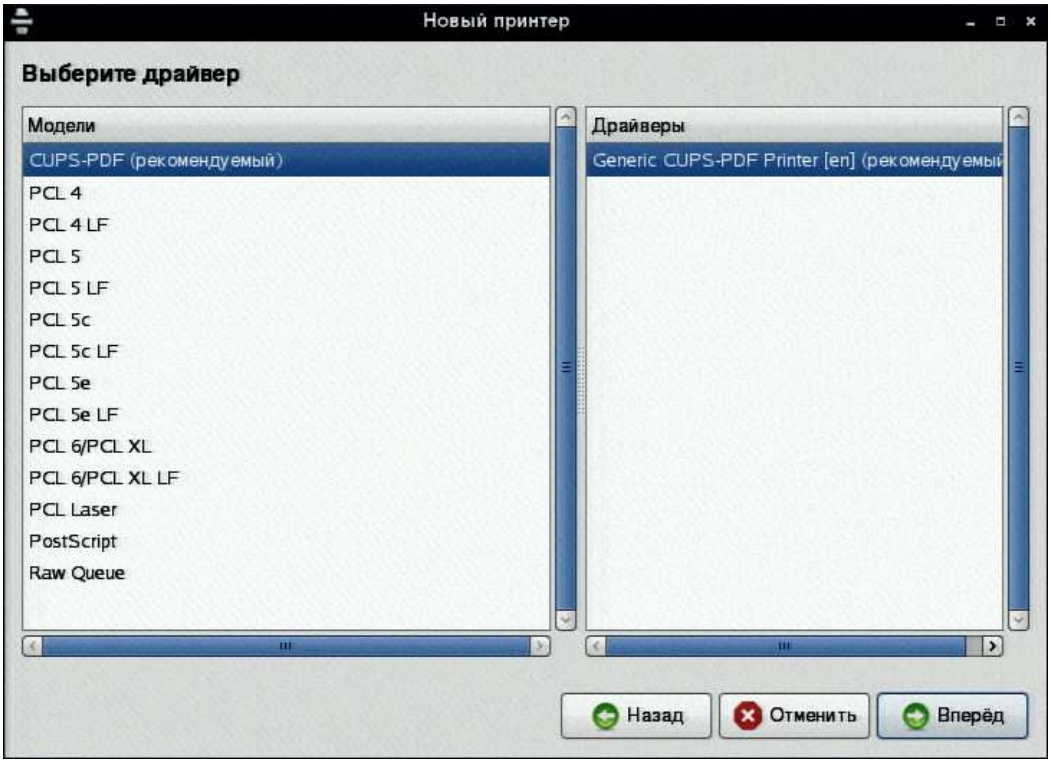


Рисунок 78 – Выбор драйвера

Далее откроется окно описания принтера (рисунок 79).

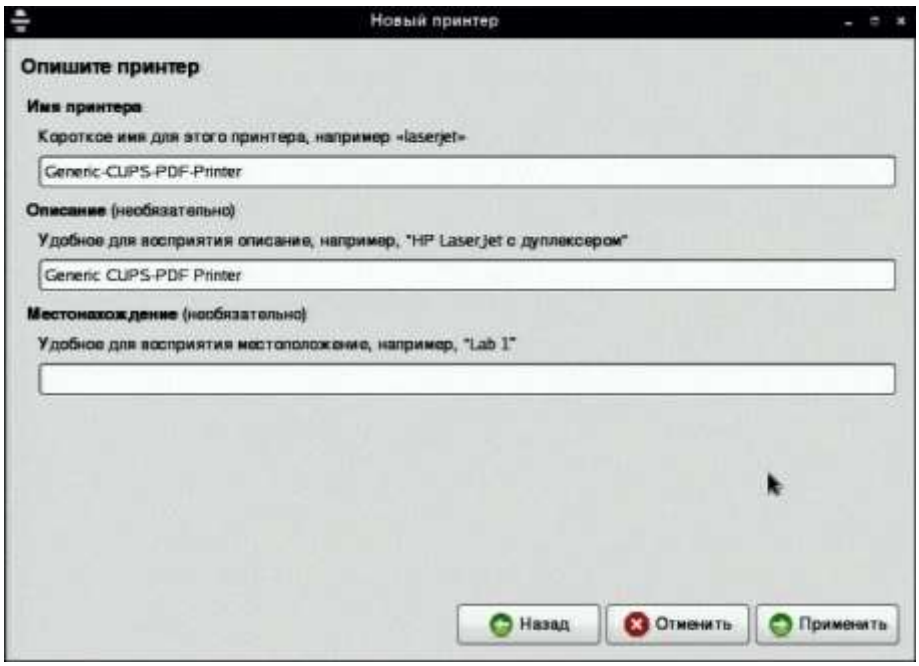


Рисунок 79 – Описание принтера

В данном окне в поле **Имя принтера** необходимо ввести короткое название для принтера.

В поле **Описание** (необязательно для заполнения) можно задать удобное описание характеристик принтера.

В поле **Местонахождение** (необязательно для заполнения) можно указать, где будет находиться принтер.

После заполнения всех необходимых полей нужно нажать кнопку **Применить**.

3.11.2 Настройка принтера

Для настройки принтера необходимо в окне менеджера принтеров (рисунок 80) нажать на принтер правой кнопкой “мыши” и в открывшемся меню выбрать пункт **Свойства**.

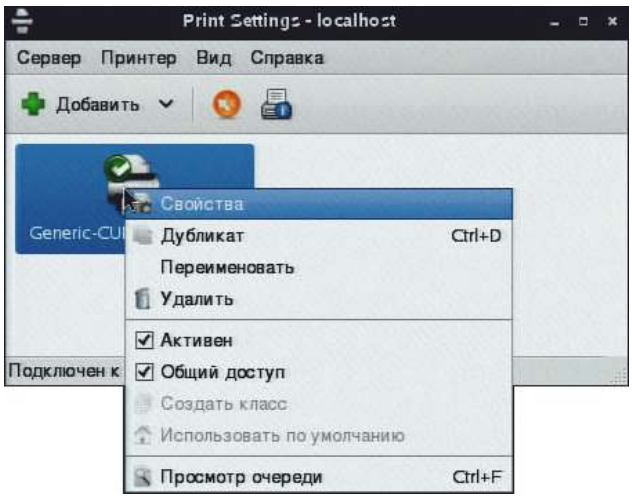


Рисунок 80 – Менеджер принтеров

Откроется окно **Свойства принтера** (рисунок 81). В левой части окна приведен список свойств принтера, а в правой – соответствующие выбранным свойствам значения.

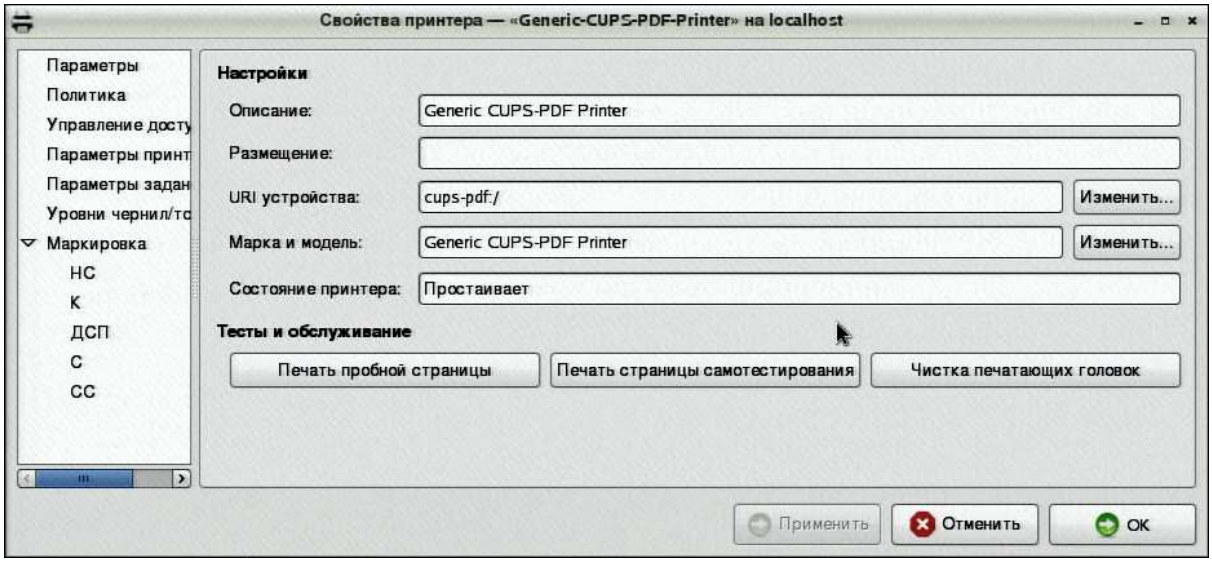


Рисунок 81 – Свойства принтера

3.11.3 Параметры

В окне **Параметры** (рисунок 81) приведены указанные при установке настройки: описание, размещение, марка и модель принтера, URI устройства и его состояние. Под заголовком **Тесты и обслуживание** находятся три кнопки:

- **Печать пробной страницы** – после нажатия будет напечатана пробная страница, позволяющая оценить, правильно ли настроен принтер.
- **Печать страницы самотестирования** – после нажатия будет напечатан отчет о состоянии принтера.
- **Чистка печатающих головок** – после нажатия запускается автоматический процесс чистки печатающих головок принтера.

3.11.3.1 Политика

В окне **Политика** (рисунок 82) можно настроить правила поведения принтера в различных ситуациях. Под заголовком **Политика** из раскрывающегося меню выбирается действие принтера при возникновении ошибок (отменять задание, повторить задание, останавливать принтер) и политика в отношении операций (требовать проверку подлинности, поведение по умолчанию).

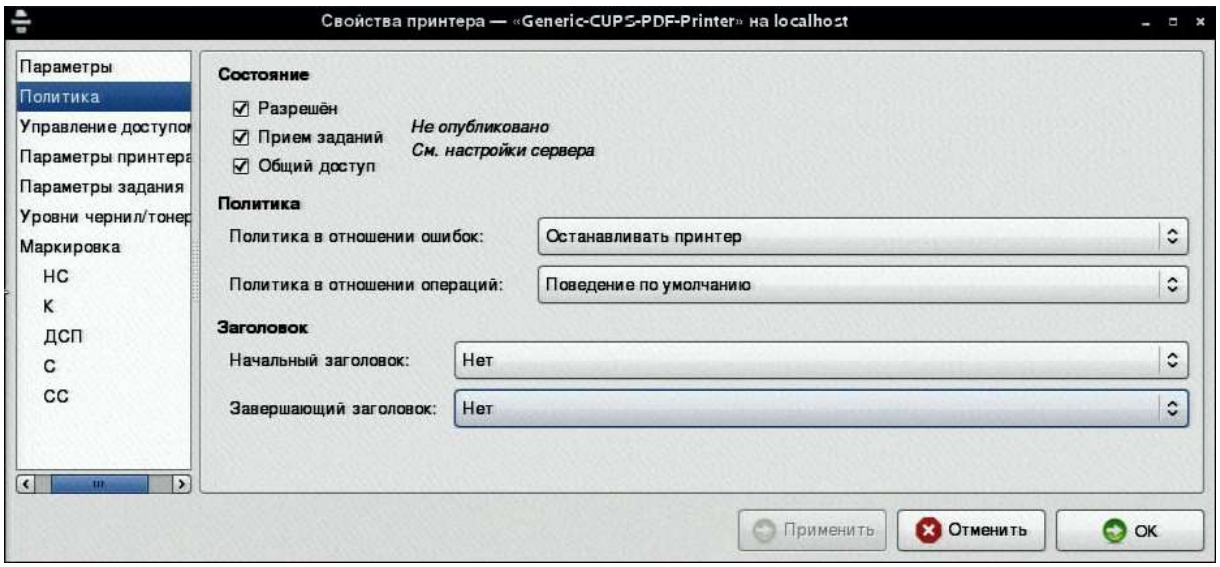


Рисунок 82 – Политика

3.11.3.2 Управление доступом

В окне **Управление доступом** (рисунок 83) настраивается доступ пользователей к принтеру:

- Разрешить печать всем, кроме указанных пользователей;
- Запретить печать всем, кроме этих пользователей.

Рисунок 83 – Управление доступом

В нижней части окна приведен список пользователей, которым в зависимости от вышеприведенных настроек разрешена или запрещена печать на принтере. Для того чтобы добавить пользователя в список, следует ввести его имя в поле и нажать кнопку **Добавить**. Чтобы удалить пользователя, нужно выделить его имя в списке и нажать кнопку **Удалить**.

3.11.3.3 Параметры принтера

В окне **Параметры принтера** (рисунок 84) настраивается размер страницы для печати и выходное разрешение.

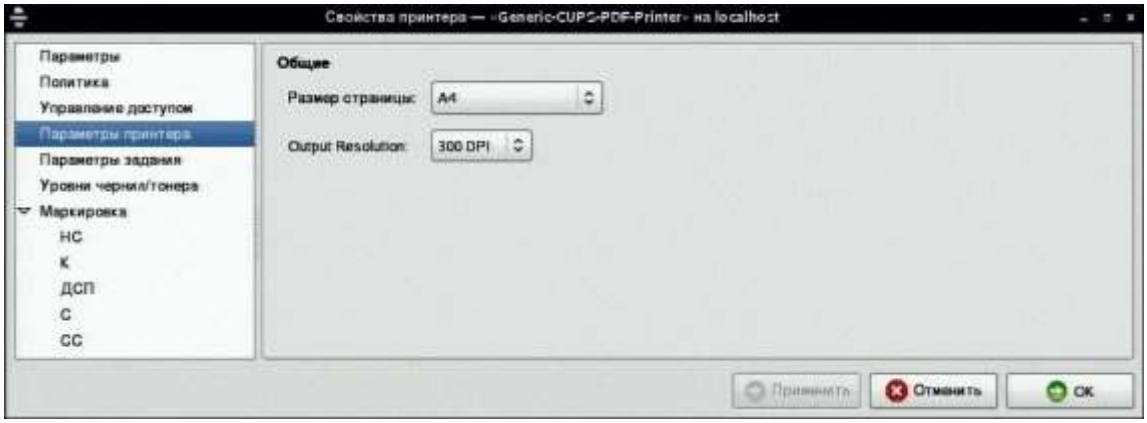


Рисунок 84 – Параметры принтера

3.11.3.4 Параметры задания

В окне **Параметры задания** (рисунок 85) указываются настройки приходящих на сервер печати заданий (файлов для печати), такие как число копий, ориентация бумаги, масштаб, размеры полей, возможность отложенной печати и другие.

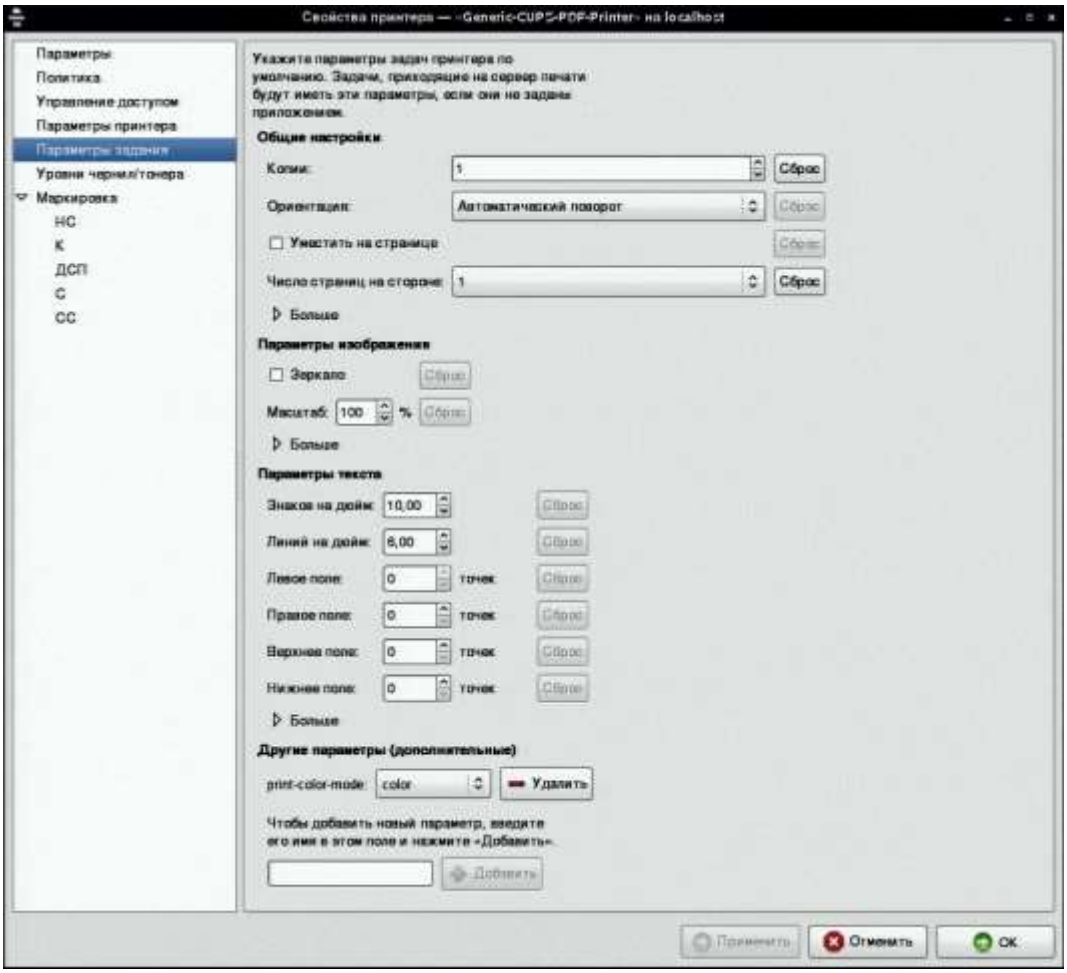


Рисунок 85 – Параметры задания

3.11.3.5 Маркировка

Администратором системы создаются мандатные категории (см. п. 3.5.1), которые используются и при печати маркированного документа.

При печати документа из *терминала* согласно мандатной метке ВМ, запущенной пользователем, в документ могут быть добавлены дополнительные специальные атрибуты. После выделения в левой части окна одной из меток конфиденциальности, в правой части появятся элементы для настройки печати документа с выбранной меткой (рисунок 86).

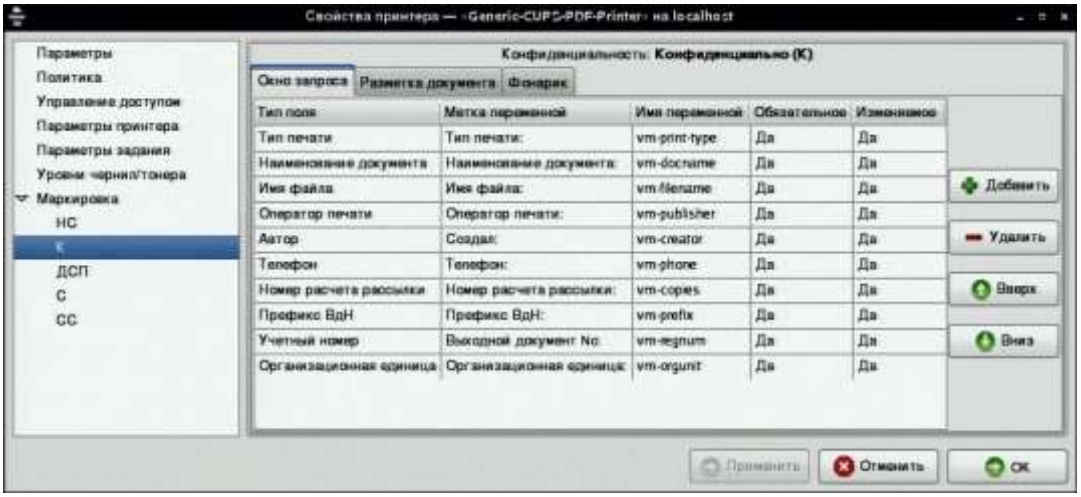


Рисунок 86 – Настройка окна запроса

На вкладке **Окно запроса** можно добавить, удалить или отредактировать поля, которые будут передаваться на терминал для ввода пользователю и затем сохраняться в системе для последующего аудита.

На вкладке **Разметка документа** (рисунок 87) можно отредактировать надписи в колонтитулах документа на первом, последнем и остальных листах (листы выбираются во вкладках окна).

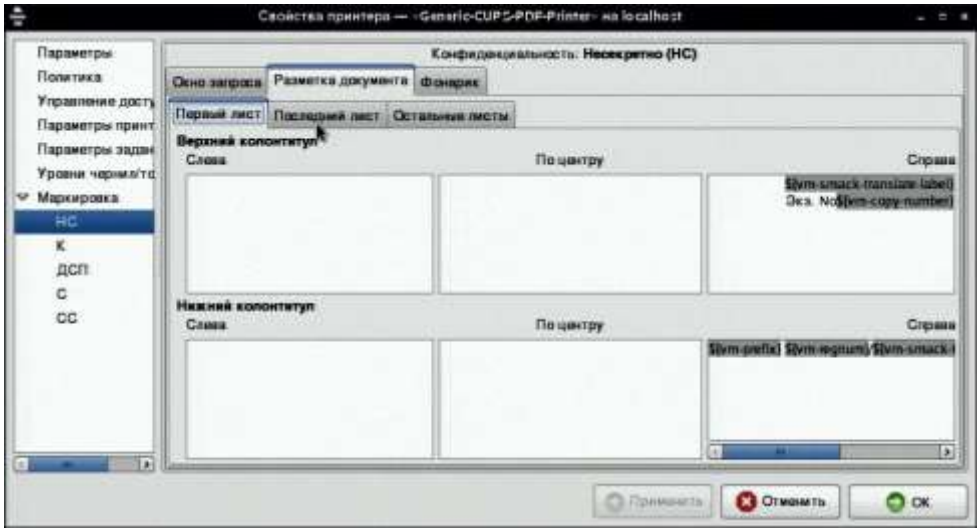


Рисунок 87 – Разметка документа

На вкладке **Фонарик** (рисунок 88) редактируется содержимое и расположение текста, который будет печататься на обратной стороне листа.

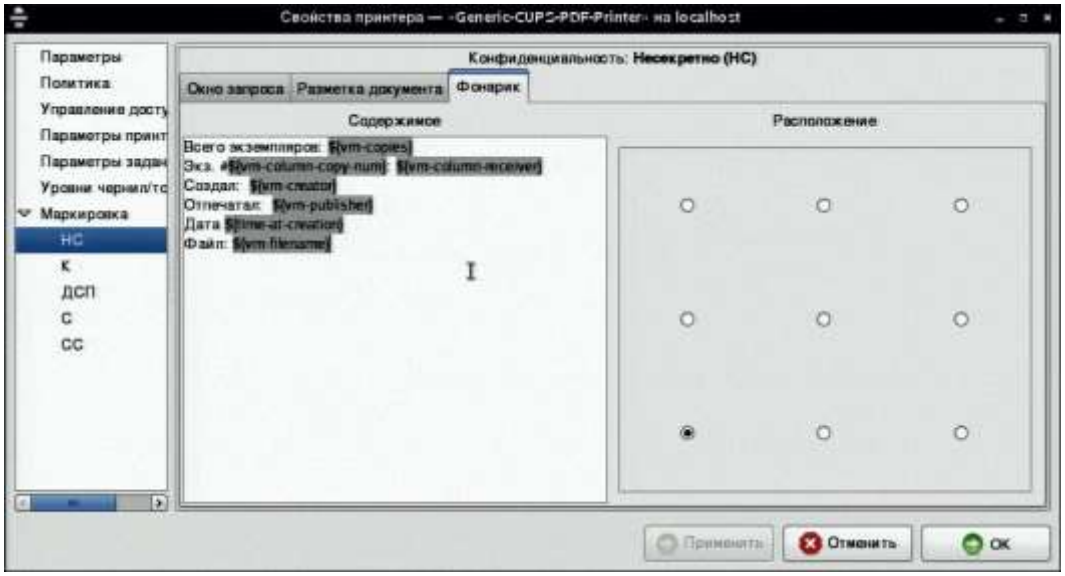


Рисунок 88 – «Фонарик»

После завершения настроек следует нажать кнопку **ОК**.

3.12 Доступ к общему хранилищу с разделением доступа по мандатному и дискреционному принципу

В системное устройство для каждой из виртуальных машин при ее создании или редактировании можно добавить устройство SAMBA, которое в гостевой операционной системе отображается как разделяемое сетевое хранилище (далее по тексту – хранилище). Каждому пользователю ПИ “Горизонт-ВС” назначается только одна ВМ, на которую назначаются мандатная метка и правила доступа. В зависимости от мандатной метки и в соответствии с описанными правилами (правила создаются и описываются администратором на сервере виртуализации), ВМ с разными метками конфиденциальности могут иметь разный уровень доступа (чтение, запись, чтение + запись) к документам на хранилище, созданным пользователями машин с иной меткой конфиденциальности. Таким образом, для пользователя, назначенного на ВМ, реализуется доступ к хранилищу с контролем по дискреционному и мандатному принципу.

Для добавления общего хранилища необходимо зайти в меню *Приложения-> Системные->Менеджер виртуальных машин*, после чего откроется окно **Менеджер виртуальных машин** (рисунок 62). Для отображения настроек необходимо кликнуть два раза левой клавишей “мыши” по иконке виртуальной машины и в открывшемся окне нажать кнопку **Показать параметры виртуального оборудования**. В окне параметров виртуального оборудования ВМ (рисунок 45) следует нажать кнопку **Добавить оборудование**.

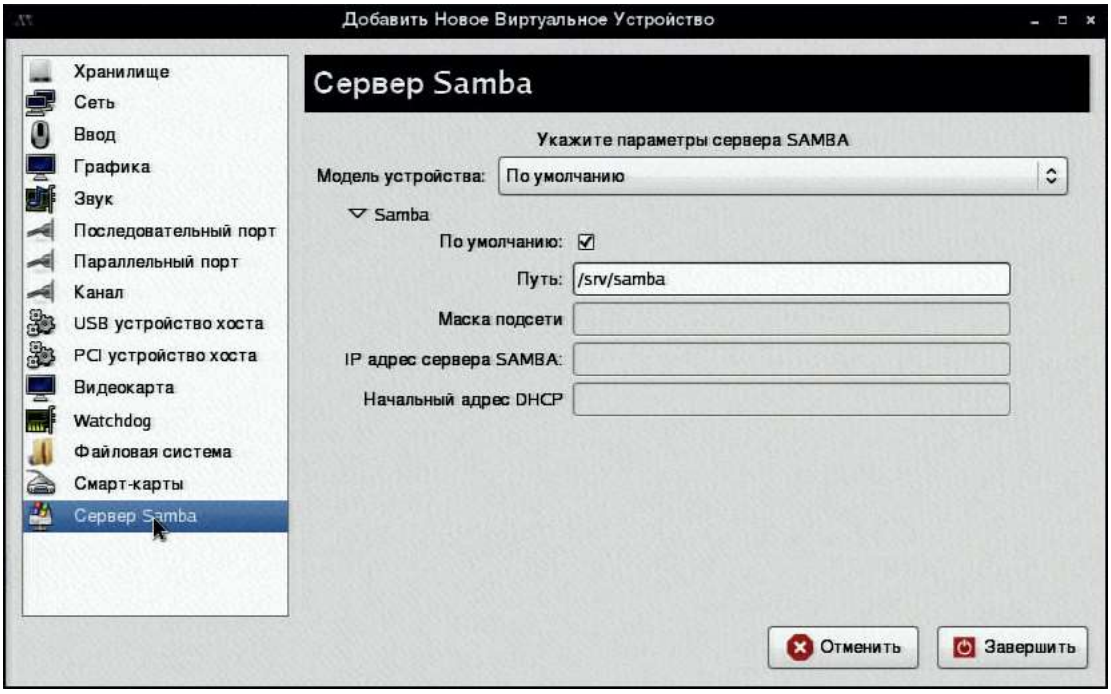


Рисунок 89 - Добавление сервера Samba

В левой части окна добавления нового виртуального устройства (рисунок 89) необходимо выбрать **Сервер Samba**.

В окне параметров хранилища необходимо выбрать модель устройства (по умолчанию, e1000, ne2k_pci, pcnet, rtl8139, virtio) и нажать кнопку **Завершить**.

Примечание: путь к серверу ***/srv/samba*** задается по умолчанию, и его невозможно изменить.

Для удаления сервера Samba следует выделить его в списке устройств в окне параметров виртуального оборудования (рисунок 45) и нажать кнопку **Удалить**.

При работе с хранилищем используется очистка памяти, механизм которой описан в Руководстве по КСЗ МБРЦ.468313.002 Д10.

3.13 Настройка параметров COM-портов

На сервере виртуализации COM-порты определяются со следующими параметрами:

ttyS0 at I/O 0x3f8 (irq = 4, base_baud = 115200) is a 16550A
ttyS1 at I/O 0x2f8 (irq = 3, base_baud = 115200) is a 16550A
ttyS2 at I/O 0x3e8 (irq = 7, base_baud = 115200) is a 16550A
ttyS3 at I/O 0x2e8 (irq = 6, base_baud = 115200) is a 16550A
ttyS4 at I/O 0x2e0 (irq = 10, base_baud = 115200) is a 16550A
ttyS5 at I/O 0x2f0 (irq = 11, base_baud = 115200) is a 16550A

В ВМ COM-порты определяются со следующими параметрами:

ttyS0 at I/O 0x3f8 (irq = 4, base_baud = 115200) is a 16550A
ttyS1 at I/O 0x2f8 (irq = 3, base_baud = 115200) is a 16550A
ttyS2 at I/O 0x3e8 (irq = 4, base_baud = 115200) is a 16550A
ttyS3 at I/O 0x2e8 (irq = 3, base_baud = 115200) is a 16550A

Необходимо привести настройку COM-портов в ВМ в соответствие с сервером виртуализации, для чего в ВМ необходимо выполнить команды:

setserial /dev/ttyS0 uart 16550A port 0x03f8 irq 4 baud_base 115200 spd_normal skip_test
setserial /dev/ttyS1 uart 16550A port 0x02f8 irq 3 baud_base 115200 spd_normal skip_test
setserial /dev/ttyS2 uart 16550A port 0x03e8 irq 7 baud_base 115200 spd_normal skip_test
setserial /dev/ttyS3 uart 16550A port 0x02e8 irq 6 baud_base 115200 spd_normal skip_test
setserial /dev/ttyS4 uart 16550A port 0x02e0 irq 10 baud_base 115200 spd_normal skip_test
setserial /dev/ttyS5 uart 16550A port 0x02f0 irq 11 baud_base 115200 spd_normal skip_test

Проверка функционирования COM-портов невозможна без специального кабеля. При его наличии соединяется два любых порта петлей и с помощью утилиты minicom (Ctrl-a o, скорость порта поставить 38400, опции в Нет Нет, сохранить и перезайти в minicom) с одной стороны и tail/echo с другой проверяются соединенные порты.

Допускается, что при такой проверке приходящие символы будут со сбитой кодировкой. При проверке с другим компьютером или оборудованием с кодировкой все должно быть в порядке при условии одинаковых настроек COM-портов.

3.14 Настройка проброса аппаратной части видеокарт в ВМ

Для добавления к ВМ видеокарты хостовой системы необходимо зайти в меню *Приложения-> Системные->Менеджер виртуальных машин*, после чего откроется окно **Менеджер виртуальных машин** (рисунок 62). Для отображения настроек необходимо кликнуть два раза левой клавишей “мыши” по иконке виртуальной машины и в открывшемся окне нажать кнопку **Показать параметры виртуального оборудования**. В окне параметров виртуального оборудования ВМ (рисунок 45) следует нажать кнопку **Добавить оборудование**.

В левой части окна добавления нового виртуального устройства необходимо выбрать **PCI устройство хоста** (рисунок 90).

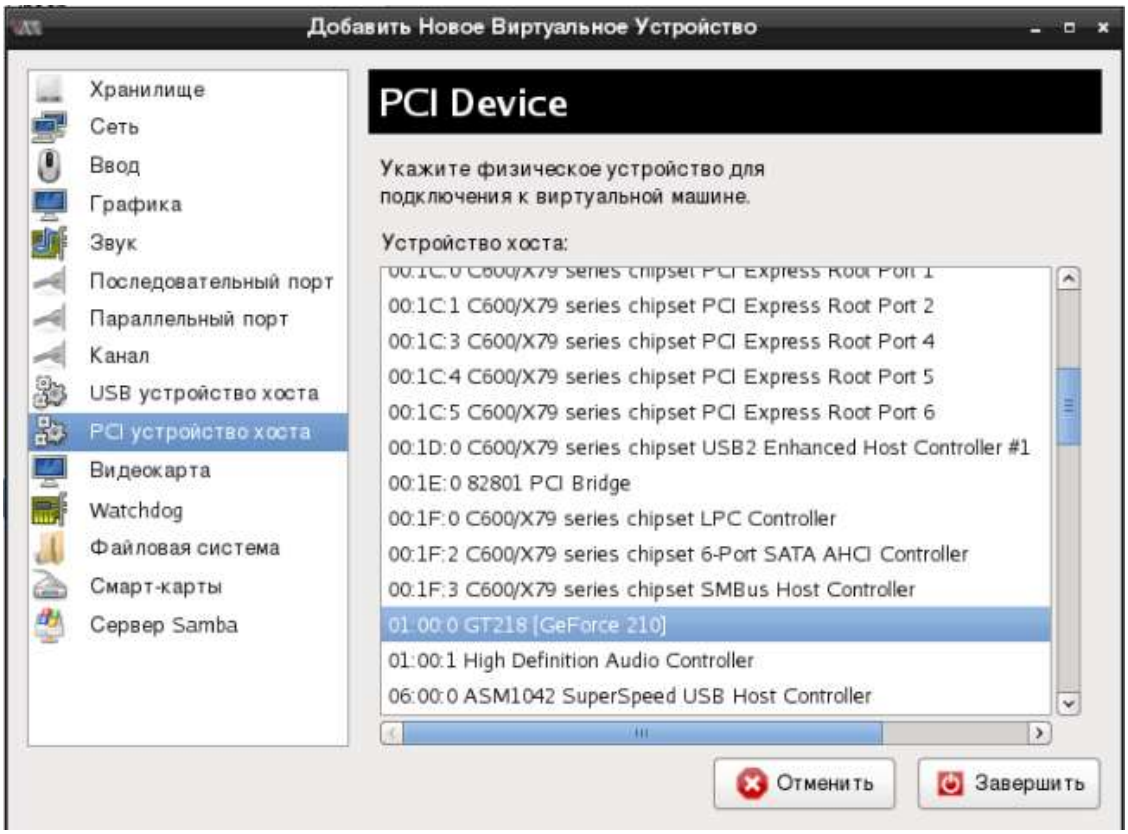


Рисунок 90 - Добавление PCI устройства в ВМ

В окне параметров необходимо выбрать модель устройства для подключения к ВМ и нажать кнопку **Завершить**.

После успешного добавления устройство будет отображено в списке (рисунок 91).

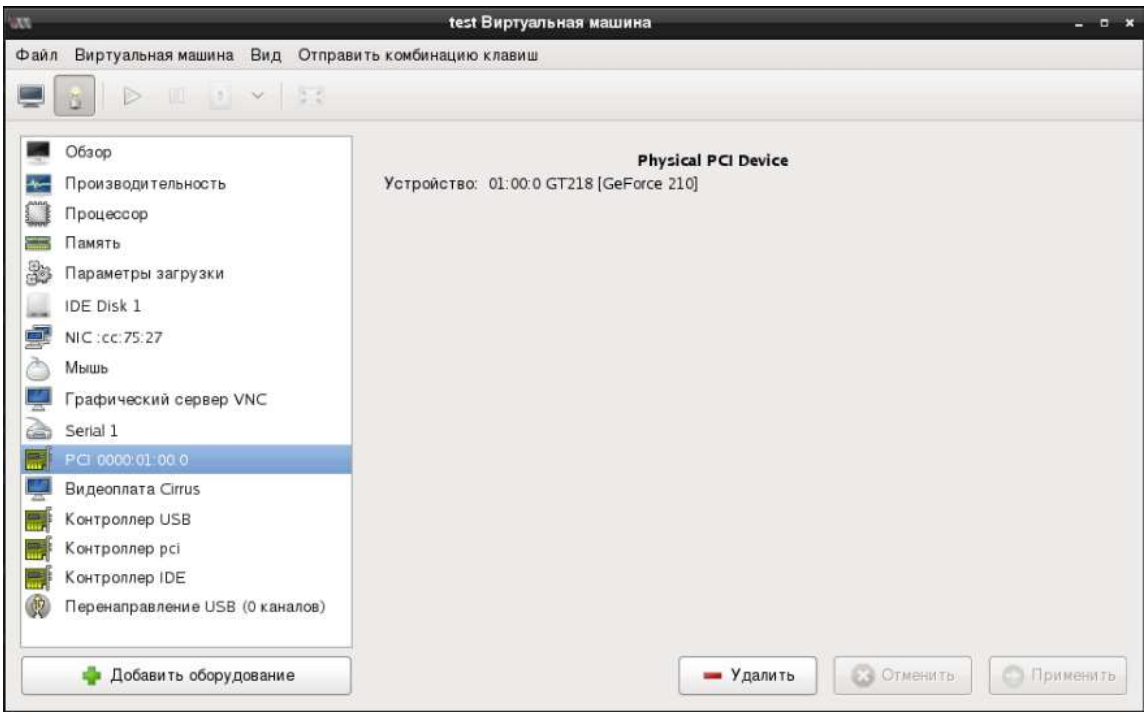


Рисунок 91

3.15 Подсистема регистрации событий

При помощи подсистемы регистрации событий можно получить подробную информацию о всех системных событиях. В ПИ “Горизонт-ВС” осуществляется регистрация следующих событий:

- использование идентификационного и аутентификационного механизма;
- запрос на доступ к защищаемому ресурсу (файл);
- создание и уничтожение файлов на общем хранилище;
- действия по изменению правил разграничения доступа (ПРД).

Настройка подсистемы регистрации событий осуществляется в файле ***/etc/audit/rules.d/audit.rules***. В начале файла размещаются несколько метаправил, задающих конфигурацию:

 # Удалить все правила из всех списков

-D

 # Указать количество буферов, хранящих сообщения аудита

-b 8192

Ниже размещаются пользовательские правила. Для того чтобы регистрировать работу пользователя с файлами на общем хранилище, а также администраторов с образами ВМ, необходимо добавить в конец файла следующие строки:

-w /srv/samba/ -p arwx

-w /var/lib/libvirt/images -p arwx

После внесения изменений в конфигурационный файл необходимо перезагрузить утилиту auditd командой в консоли:

service auditd restart

3.15.1 Получить сведения об идентификации и аутентификации пользователей можно, набрав в консоли команду

cat /var/log/messages | grep vmacd

В результате в консоль будут выведены сообщения следующего типа (рисунки 92, 93):

- в случае успешной аутентификации – ***User <****имя пользователя****> request connect***;
- в случае неуспешной аутентификации – ***SASL: performing SASL negotiation: authentication failure***;
- при попытке аутентификации незарегистрированного пользователя – ***SASL: performing SASL negotiation: user not found***.

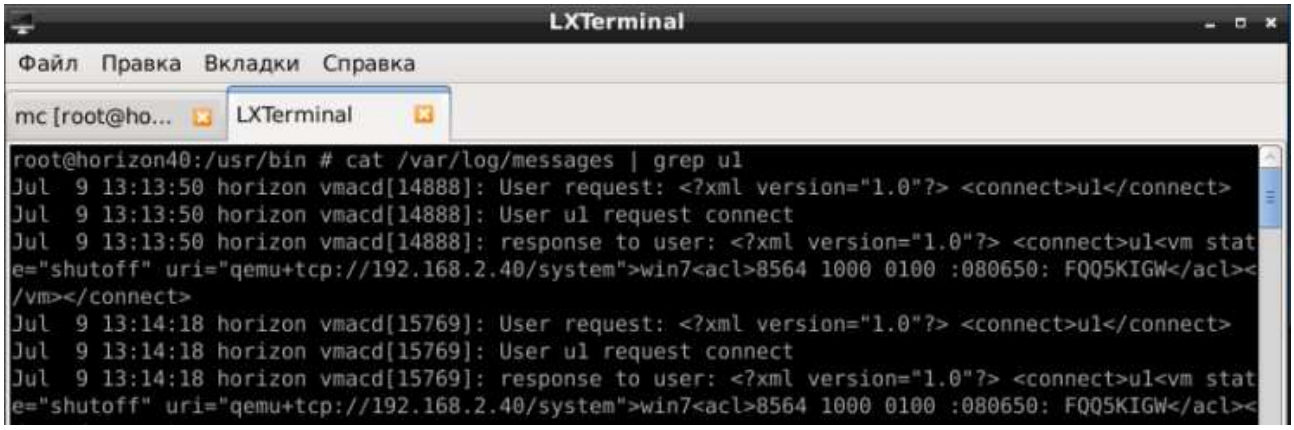


Рисунок 92

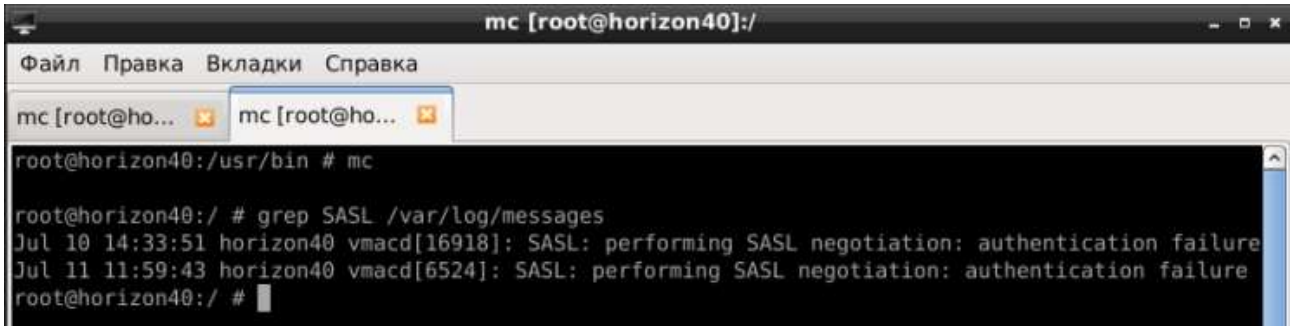


Рисунок 93

3.15.2 Данные о доступе

Данные создании пользователем файла можно получить командой:

ausearch –ua <*UID пользователя****> --interpret | grep CREATE***

где значение *UID пользователя* можно получить, используя команду: ***id*** *<имя пользователя в системе>*.

Команда отображает подробную информацию по выбранному событию:

- дата и время (msg=audit),
- название файла (name),
- пользователь (ouid) и группа (ogid),
- успешность выполнения (success=no/yes).

Данные об удалении пользователем файла можно получить командой:

ausearch –ua <*UID пользователя****> --interpret | grep DELETE***

где значение *UID пользователя* можно получить, используя команду: ***id*** *<имя пользователя в системе>*.

Данные об изменении правил разграничения доступа можно получить командой в консоли:

ausearch -ua <*UID пользователя****> --interpret | grep chown***

или

ausearch -ua <*UID пользователя****> --interpret | grep chmod***

где значение *UID пользователя* можно получить, используя команду: ***id*** *<имя пользователя в системе>*.

Размер журнала регистрации событий ограничен 6 Мб. После превышения данного размера осуществляется перезапись журнала.

Тестирование журнала на переполнение осуществляется командами из консоли:

auditctl –a exit,always –S open

auditctl –a exit,always –S execve

ВНИМАНИЕ. После окончания проверки следует ввести в консоли команду ***auditctl –D***, которая отменяет созданные ранее правила.

Тестирование выполняется около 5-ти минут. При превышении журналом аудита размер 6 Мб осуществляется перезапись.

3.15.3 Очистка журнала регистрации событий

Очистка журнала регистрации событий производится удалением файлов ***/var/log/audit/audit.log*** и ***var/log/messages*** на сервере виртуализации.

3.16 Миграция

Миграция — перенос виртуальной машины с одного физического сервера на другой без прекращения работы виртуальной машины и остановки сервисов.

ВНИМАНИЕ. Миграция может осуществляться только при наличии iSCSI или NFS хранилища, содержащем образ ВМ, которую необходимо мигрировать. Также режим кэширования диска ВМ должен быть установлен в “**none**” (см. раздел 3.7.6, рисунок 50).

Сервер виртуализации, с которого будет осуществляться миграция, будем называть исходным сервером виртуализации. Сервер виртуализации, на которой будет осуществляться миграция, назовем сервером миграции.

Перед началом настроек необходимо внести изменения в файл ***libvirtd.conf***, находящийся по адресу: */etc/libvirt/libvirtd.conf*:

listen_tls = 0

listen_tcp = 1

auth_tcp = “none”

auth_tls = “none”

В файле */etc/sysconfig/libvirtd* необходимо убрать комментарий (#) и в консоли перезапустить сервис libvirtd командой: ***service libvirtd restart***.

Также следует на обоих серверах в файл /etc/hosts внести информацию об именах серверов, добавив в конец строки вида:

<*ip-адрес сервера исходного сервера виртуализации****> <****DNS имя сервера исходного сервера виртуализации****>***

<*ip-адрес сервера миграции****> <****DNS имя сервера миграции****>***

DNS имя сервера задается на вкладке "DNS" в окне **Настройка сети** (рисунок 25).

На сервере миграции должен быть создан пользователь с тем же именем, что и назначенный на ВМ на исходном сервере виртуализации.

3.16.1 Настройка подключения к iSCSI хранилищу.

В консоли от имени администратора следует ввести команду:

iscsiadm –m discovery –t st –p <*ip хранилища****>***

В ответ будет выведена строка следующего вида:

<*ip хранилища****>:3260,1 iqn.<****имя хранилища****>:<****имя ВМ****>***

Для того чтобы добавить iSCSI хранилище, необходимо в **Менеджере виртуальных машин** (рисунок 62) выбрать пункт меню *Правка->Свойства подключения* и в открывшемся окне **Свойства соединения** (рисунок 94) выбрать вкладку **Хранилище**. В нижней части окна следует нажать кнопку **Добавить пул**.

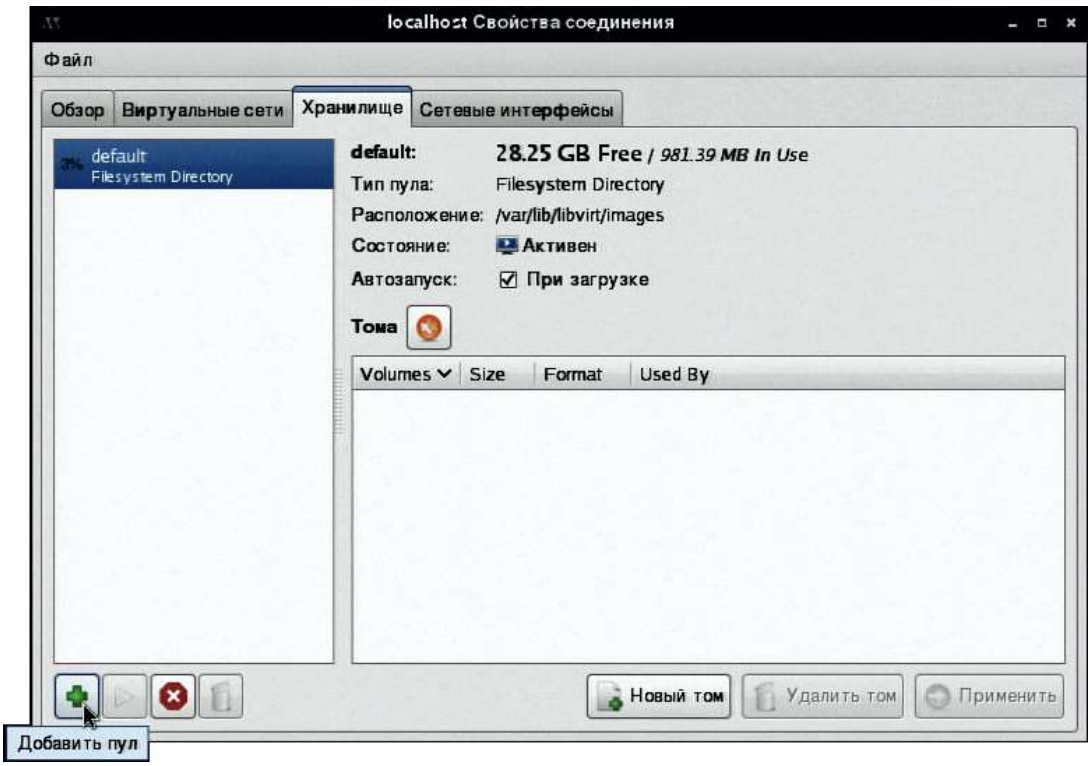


Рисунок 94 – Свойства соединения. Хранилище

В следующем окне (рисунок 95) необходимо ввести название ВМ и из раскрывающегося списка выбрать тип – **iscsi: ISCSI Target**. Нажать кнопку **Вперед**.

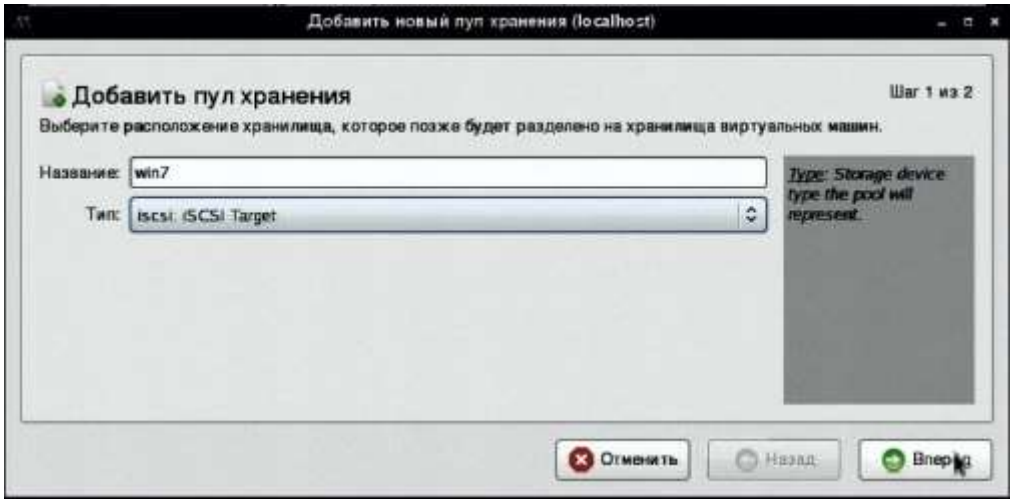


Рисунок 95 – Добавление пула хранения. Шаг 1

На следующем шаге следует в поле **Имя хоста** необходимо ввести ip-адрес хранилища, а в поле **Путь к источнику** – ***iqn.<имя хранилища>:<имя ВМ>***, полученные выше в консоли, и нажать кнопку **Завершить** (рисунок 96).

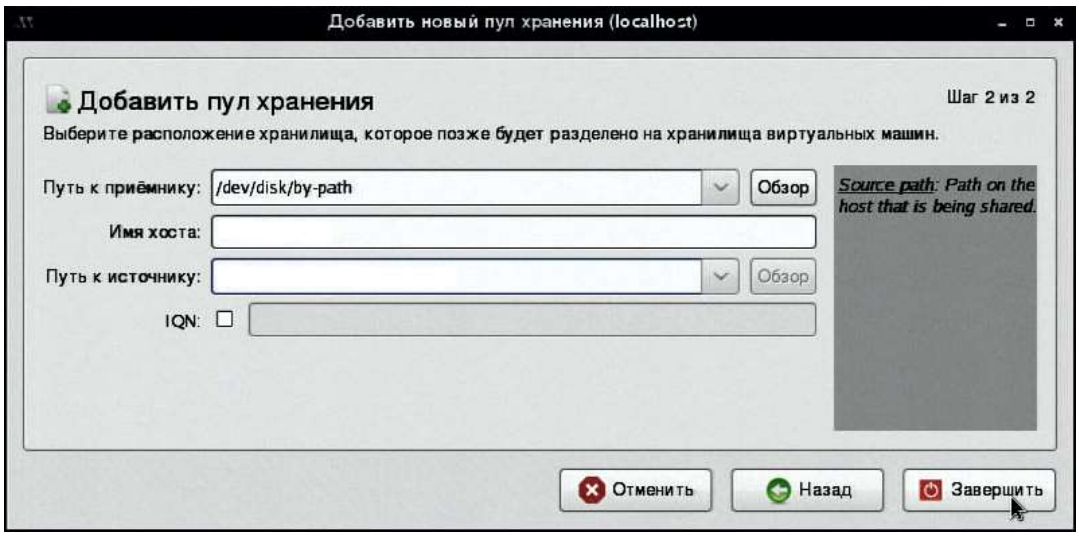


Рисунок 96 – Добавление пула хранения. Шаг 2

После этого созданное хранилище появится в левой части окна **Свойства соединения** (рисунок 94).

3.16.2 Настройка подключения NFS хранилища

На сервере виртуализации, с которого будет осуществляться миграция, в файле ***/etc/exports*** следует ввести строку следующего вида:

<**директория с образом ВМ**> <**ip-адрес сервера миграции**>(rw,no_root_squash,no_subtree_check)

Примечание: путь к директории, где хранится образ ВМ, на исходном сервере виртуализации и на сервере миграции должен быть полностью идентичен.

В консоли исходного сервера виртуализации от имени администратора ввести команду запуска NFS хранилища:

/etc/rc.d/init.d/nfs-server start

Все выводимые в консоль ответные сообщения должны иметь статус “OK”.

На сервере миграции в файле ***/etc/fstab*** ввести строку следующего вида:

<**ip-адрес сервера исходного сервера виртуализации**> <**директория с образом ВМ на сервере виртуализации**> <**директория с образом ВМ на сервере миграции**>

На сервере миграции примонтировать NFS хранилище командой в консоли:

mount.nfs <**ip-адрес сервера исходного сервера виртуализации**>:<**директория с образом ВМ**> <**директория с образом ВМ на сервере миграции**>

3.16.3 Создание соединения с удаленным сервером

Для создания соединения с удаленным сервером в **Менеджере виртуальных машин** (рисунок 62) необходимо нажать пункт меню *Файл->Добавить соединение* (рисунок 97).

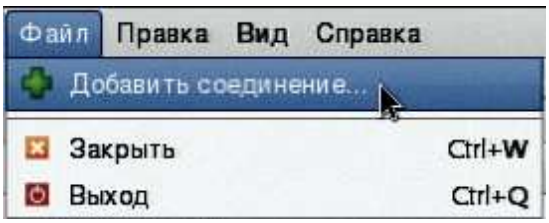


Рисунок 97 – Создание соединения

В появившемся окне (рисунок 98) необходимо установить следующие параметры. Из раскрывающегося меню **Гипервизор** выбрать значение ***QEMU, KVM*** (по умолчанию), установить флажок **Подключиться к удаленному хосту**; из раскрывающегося меню **Тип** выбрать значение ***TCP***; ввести в поле **Имя пользователя** – ***vss*** (по умолчанию), **Имя хоста** – адрес или название удаленного сервера. После нажатия кнопки **Подключиться** в менеджере будет создано новое соединение.

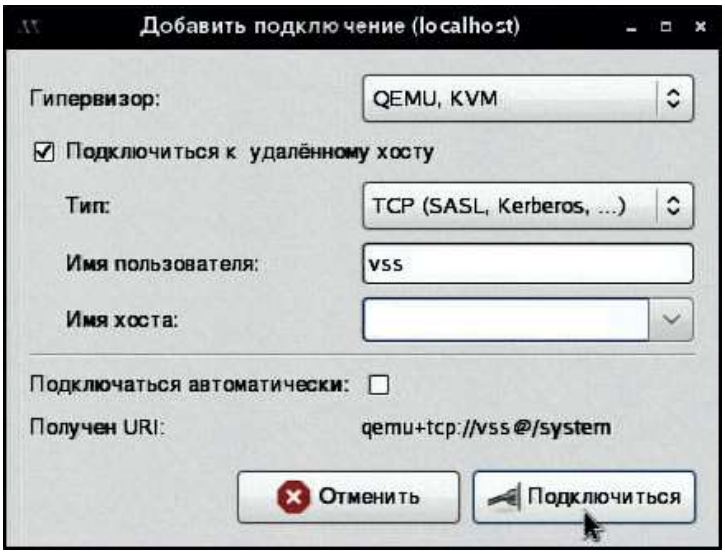


Рисунок 98 – Добавление подключения

Для подключения к серверу ВМ необходимо в Менеджере виртуальных машин (рисунок 35) на соединении с сервером нажать правую клавишу “мыши” и выбрать пункт **Подключиться**.

Для отключения от сервера ВМ необходимо в Менеджере виртуальных машин (рисунок 35) на соединении с сервером нажать правую клавишу “мыши” и выбрать пункт **Отключиться**.

Для удаления соединения с сервером ВМ необходимо в Менеджере виртуальных машин (рисунок 35) на соединении с сервером, нажать правую клавишу “мыши” и выбрать пункт **Удалить**.

3.16.4 Миграция на удаленный сервер ВМ

Для выполнения процедуры миграции необходимо в Менеджере виртуальных машин (рисунок 35) кликнуть на иконке запущенной ВМ правой клавишей мыши и вы-

брать пункт “**Миграция…**”. В появившемся окне (рисунок 99) в поле **Новый хост** из раскрывающегося списка выбрать сервер ВМ, на который будет осуществляться процедура миграции. После выбора сервера необходимо нажать кнопку **Миграция**.

Примечание. В дополнительных параметрах рекомендуется установить флажок **Макс. Выключено** и ввести значение временного интервала от 300 до 500 мс для ускорения процесса миграции.

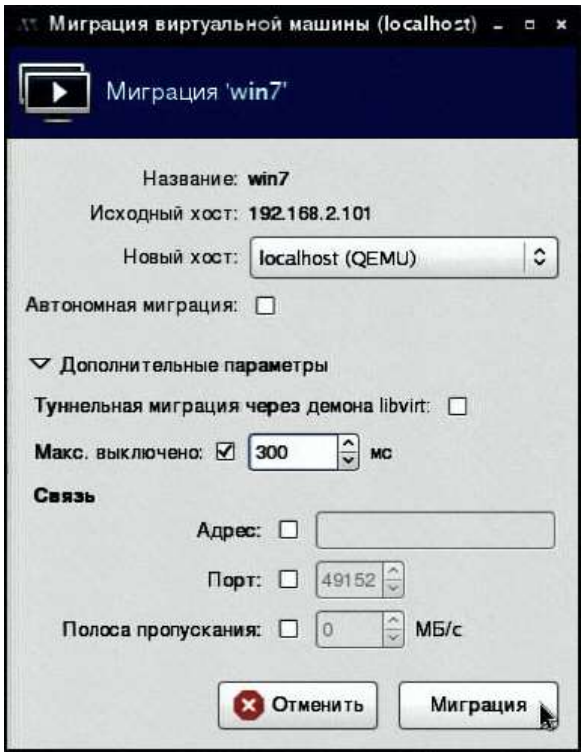


Рисунок 99 – Миграция ВМ

3.16.5 Миграция виртуальных машин без общего хранилища

Для осуществления «живой» миграции ВМ при использовании локального хранилища необходимо перед началом миграции скопировать виртуальный диск ВМ на сервер миграции командой в консоли:

$ scp /var/lib/libvirt/images/<имя_ВМ>.img <ip-адрес_сервера_миграции>:/var/lib/libvirt/images/<имя_ВМ>.img

И затем выполнить команду миграции ВМ:

$ virsh migrate --live -p2p --persistent --verbose --copy-all --undefinesource <имя_ВМ> qemu+ssh://<имя_сервера_виртуализации>/system

После окончания процесса миграции работающая ВМ переместится на сервер миграции.

3.17 Настройка DRBD

DRBD (Distributed Replicated Block Device — распределённое реплицируемое блочное устройство) — это блочное устройство, предназначенное для построения отказоустойчивых кластерных систем. DRBD занимается полным отражением (mirroring) по сети всех операций с блочным устройством.

Для настройки DRBD необходимо создать следующие конфигурационные файлы:

1. Файл, расположенный в директории ***/etc/drbd.d/global_common.conf***, следует заполнить следующим образом:

```
# DRBD is the result of over a decade of development by LINBIT.
  # In case you need professional services for DRBD or have
  # feature requests visit http://www.linbit.com
  global {
      usage-count no;
      disable-ip-verification;
      # minor-count dialog-refresh disable-ip-verification
      # cmd-timeout-short 5; cmd-timeout-medium 121; cmd-timeout-long 600;
  }
  common {
          handlers {
                  # These are EXAMPLE handlers only.
                  # They may have severe implications,
                  # like hard resetting the node under certain circumstances.
                  # Be careful when chosing your poison.

                  pri-on-incon-degr "/usr/lib/drbd/notify-pri-on-incon-degr.sh;
/usr/lib/drbd/notify-emergency-reboot.sh; echo b > /proc/sysrq-trigger ; reboot -f";
                  pri-lost-after-sb "/usr/lib/drbd/notify-pri-lost-after-sb.sh;
/usr/lib/drbd/notify-emergency-reboot.sh; echo b > /proc/sysrq-trigger ; reboot -f";
                  local-io-error "/usr/lib/drbd/notify-io-error.sh; /usr/lib/drbd/notify-
emergency-shutdown.sh; echo o > /proc/sysrq-trigger ; halt -f";
                  # fence-peer "/usr/lib/drbd/crm-fence-peer.sh";
                  split-brain "/usr/lib/drbd/notify-split-brain.sh root";
                  initial-split-brain "/usr/lib/drbd/notify-split-brain.sh root";
                  out-of-sync "/usr/lib/drbd/notify-out-of-sync.sh root";
                  # before-resync-target "/usr/lib/drbd/snapshot-resync-target-lvm.sh -p
15 -- -c 16k";
                  # after-resync-target /usr/lib/drbd/unsnapshot-resync-target-lvm.sh;
          }

          startup {
                  # wfc-timeout degr-wfc-timeout outdated-wfc-timeout wait-after-sb
          }

          options {
                  # cpu-mask on-no-data-accessible
          }

          disk {
                  fencing dont-care;
                  # on-io-error call-local-io-error;
                  # disk-drain md-flushes resync-rate resync-after al-extents
                  c-plan-ahead 150;
                  # c-delay-target
```

```
                c-fill-target 40M;
                c-max-rate 700M;
                c-min-rate 4M;
                # disk-timeout
                on-io-error detach;
        }

        net {
                protocol C;
                # timeout
                max-epoch-size 8192;
                max-buffers 12000;
                # unplug-watermark
                # connect-int ping-int
                sndbuf-size 2097152;
                rcvbuf-size 2097152;
                # ko-count
                # allow-two-primaries cram-hmac-alg shared-secret after-sb-0pri
                # after-sb-1pri after-sb-2pri always-asbp rr-conflict
                # ping-timeout
                data-integrity-alg sha1;
                # tcp-cork on-congestion
                # congestion-fill congestion-extents
                csums-alg sha1;
                # verify-alg
                # use-rle
                after-sb-0pri discard-zero-changes;
                after-sb-1pri discard-secondary;
                after-sb-2pri violently-as0p;
        }  }
```

2. Файл, расположенный в директории ***/etc/drbd.d/<RESOURCE NAME>.res***, описывающий реплицируемые блочные устройства и узлы, участвующие в процессе, следует заполнить следующим образом:

```
resource <RESOURCE NAME> {
      on <node_name_A> {
          # device to create
          device    /dev/drbd1;
          # low-level device
          disk      /dev/disk/by-id/wwn-0x600140580040c51b41a4bc2ae5e57528;
          # unique replication uri
          address   <IP_address_A>:7789;
          meta-disk internal;
      }
      on <node_name_B> {
          device    /dev/drbd1;
          disk      /dev/disk/by-id/wwn-0x6001405f0657c3d2e0946d69857e2de5;
          address   <IP_address_B>:7789;
          meta-disk internal;
      }
  }
```

где в секции *<node_name_XX> {…}* на каждом из узлов будут применены настройки, соответствующие имени узла (информацию об узле можно узнать командой ***uname -n***):

- параметр *address* содержит IP-адрес данного узла;

– параметр *device* указывает устройство, создаваемое подсистемой DRBD, доступное для использования в системе и обеспечивающее репликацию записываемых данных.

– параметр *disk* – блочное устройство, подлежащее репликации; при активации подсистемы DRBD перестаёт быть доступным для операций чтения/записи.

После заполнения конфигурационные файлы ***global_common.conf*** и ***/<RESOURCE NAME>.res*** следует скопировать на второй узел репликации.

На каждом узле выполнить команду в консоли для создания метаданных реплицируемого ресурса:

drbadm create-md <*RESOURCE NAME****>***

Включить ресурс на каждом узле выполнением команды в консоли:

drbadm up <*RESOURCE NAME****>***

Запустить начальную синхронизацию:

drbadm primary --force <*RESOURCE NAME****>***

За ходом синхронизации можно следить с помощью команды ***cat /proc/drbd*** или ***watch -n1 cat /proc/drbd***.

3.18 Настройка кластера Pacemaker/Corosync

На всех серверах виртуализации, являющимися узлами кластера, должна быть возможность получить IP-адрес по имени узла. Для этого либо DNS, либо IP-адреса и имена всех узлов должны быть прописаны в файле ***/etc/hosts*** единым образом на всех узлах кластера.

На всех узлах кластера необходимо остановить и удалить из автозагрузки службы corosync-notifyd и pacemaker_remote:

service corosync-notifyd stop
service pacemaker_remote stop
chkconfig --del corosync-notifyd
chkconfig --del pacemaker_remote

3.18.1 Настройка Corosync

Corosync служит транспортным уровнем кластера, также на этом уровне обеспечивается кворум. Этот уровень может быть сконфигурирован двумя различными способами.

Первый способ предусматривает использование multicast протокола и при большом количестве узлов может быть менее эффективным, однако не требует указания IP-адресов узлов, и, следовательно, переконфигурации в случае изменения последних.

Второй способ использует unicast протокол и требует перечисления в конфигурации corosync всех узлов кластера.

Настройка состоит из следующих последовательных шагов:

1. На одном из узлов кластера создать конфигурационный файл ***/etc/corosync/corosync.conf***.
   - для multicast протокола. Содержимое можно взять из файла ***/etc/corosync/corosync.conf.example***. Должно получиться следующее содержимое файла:

```
totem {
        version: 2
        crypto_cipher: none
        crypto_hash: none
        cluster_name: Name
        interface {
                ringnumber: 0
                bindnetaddr: <net_address>
                mcastaddr: 239.255.1.1
                mcastport: 5405
                ttl: 1
        }
} logging {
        fileline: off
        to_stderr: no
        to_logfile: yes
        logfile: /var/log/cluster/corosync.log
        to_syslog: yes
        debug: off
        timestamp: on
        logger_subsys {
                subsys: QUORUM
                debug: off
        }
} quorum {
  provider: corosync_votequorum
  two_node: 1
  expected_votes: 1
```

}

Секция *totem.interface* определяет интерфейс, используемый узлами для служебного трафика кластера, в случае резервирования каналов связи таких секций может быть несколько. Их идентификация и приоритет использования определяется параметром *totem.interface.ringnumber*, который должен принимать значения, начиная с 0, и инкрементироваться на 1. Он должен совпадать для соответствующих сетей у всех узлов кластера.

Параметр *totem.interface.bindnetaddr* должен соответствовать адресу сети, к которой подключен интерфейс.

Параметр *totem.interface.mcastaddr* – выделенный multicast-адрес для кластера.

Параметр *totem.interface.mcastport* – выделенный multicast-порт для кластера.

Параметр *quorum.two_nodes* контролирует возможность создания кластера из двух узлов.

Примечание – параметр quorum.expected_votes должен отражать необходимое количество запущенных узлов для начальной инициализации кластера.

– для unicast протокола содержимое можно взять из файла ***/etc/corosync/corosync.conf.example.udpu***. Должно получиться следующее содержимое файла:

```
totem {
        version: 2
        crypto_cipher: none
        crypto_hash: none
        cluster_name: Name
        interface {
                ringnumber: 0
                bindnetaddr: <net_address>
                mcastport: 5405
                ttl: 1
        }
        transport: udpu
} logging {
        fileline: off
        to_stderr: no
        to_logfile: yes
        logfile: /var/log/cluster/corosync.log
        to_syslog: yes
        debug: off
        timestamp: on
        logger_subsys {
                subsys: QUORUM
                debug: off
        }
} nodelist {
  node {
```

```
        ring0_addr: <node_ip_addr_in_ring0_interface_network>
        nodeid: 1
    }
} quorum {
    provider: corosync_votequorum
    two_node: 1
}
```

Необходимо внести следующие изменения:

- параметр *totem.interface.mcastaddr* не нужен;
- параметр *totem.transport* должен быть установлен в значение udpu;
- *quorum.expected_votes* необходимо убрать;
- должна присутствовать секция nodelist с подсекциями nodelist.node для каждого узла кластера;
- для каждого узла кластера должен быть указан его IP-адрес в параметре *nodelist.node.ring<X>_addr: <IP_address>* соответствующий одному из интерфейсов кластера сконфигурированному в секции *totem.interface* с параметром *ringnumber* равным <X>;
- для каждого узла кластера параметр *nodelist.node.nodeid* должен быть уникален.

2. Скопировать созданный конфигурационный файл на все узлы кластера.
3. Запустить на всех узлах кластера службу corosync командой:

service corosync start

4. Проконтролировать работу транспортного уровня командой:

corosync-quorumtool

в выводе которой должны присутствовать все узлы кластера.

3.18.2 Настройка Pacemaker

Настройка состоит из следующих последовательных шагов:

1. Запустить на всех узлах кластера службу pacemaker командой

service pacemaker start

2. Проконтролировать состояние кластера командой

crm status

в выводе которой должны присутствовать все узлы кластера, и полное отсутствие выполняемых ресурсов.

3.19 Работа с системой резервирования ВМ

Для организации периодического сохранения конфигураций ВМ, дисков ВМ, конфигураций “снимков” работающих ВМ, исполняющихся на сервере виртуализации, а также конфигураций виртуальных сетей предназначена программа “СРВМ”. Сохранение данных производится централизованно на единой ПЭВМ – сервере резервирования.

Так как сборка КП “Терминал-Сервер” и программы “СРВМ” осуществляется совместно, отдельной установки и настройки системы резервирования не требуется.

После первого запуска или перезапуска сервера виртуализации следует проверить, что программа “СРВМ” запущена, путем набора команды в консоли:

service gbs_ftpd status

Результатом должно быть значение – *active [running]*. Если программа отключена, следует запустить её командой в консоли:

service gbs_ftpd start

После запуска сервера резервирования на нем следует запустить программу “СРВМ” командой в консоли:

service gbs_mand start

После этого начнется процесс синхронизации.

В графическом виде данные программы “СРВМ” можно посмотреть, выполнив команду в консоли: ***gbsgui***, после чего откроется окно как на рисунке 100.

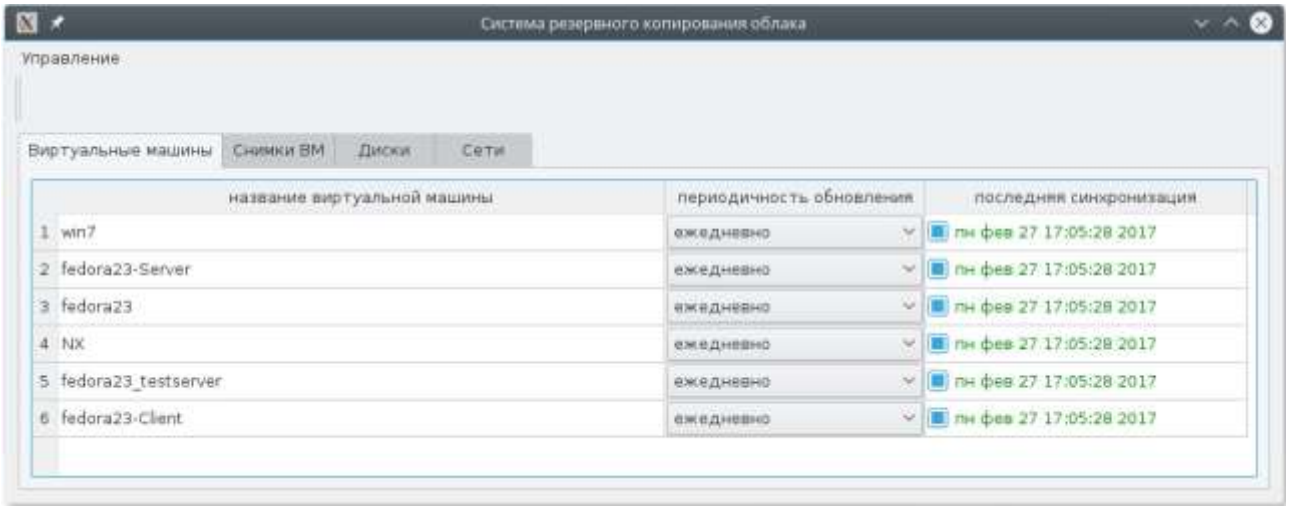


Рисунок 100 - "СРВМ". Виртуальные машины

На вкладке **Виртуальные машины** в первом столбце перечислены названия ВМ, резервные копии конфигураций которых хранятся на сервере резервирования; во

втором – периодичность обновления, в третьем – дата и время последней синхронизации.

На вкладке **Снимки ВМ** (рисунок 101) в первом столбце перечислены названия ВМ, резервные копии “снимков” которых хранятся на сервере резервирования; во втором – название “снимка” ВМ, в третьем – периодичность обновления, в четвертом – дата и время последней синхронизации.

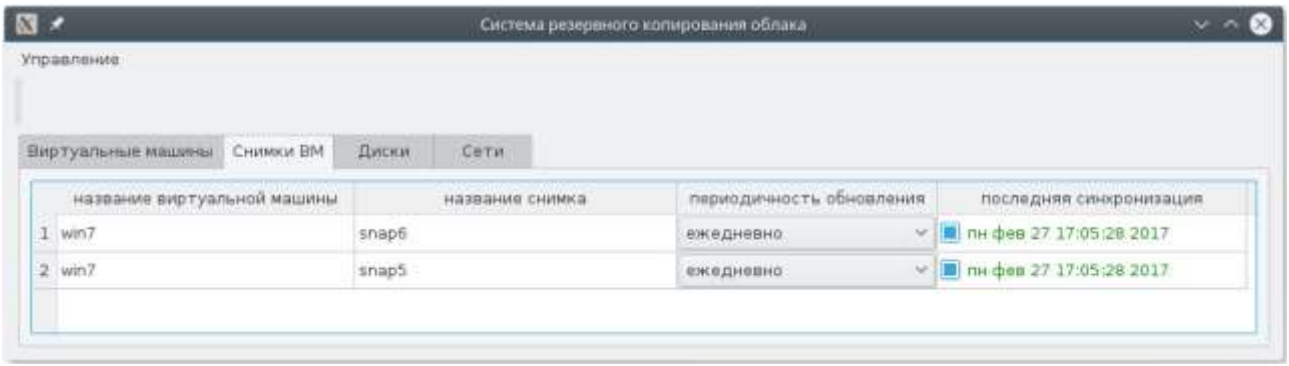


Рисунок 101 - "СРВМ". Снимки ВМ

На вкладке **Диски** (рисунок 102) в первом столбце в первом столбце перечислены названия ВМ, резервные копии дисков которых хранятся на сервере резервирования; во втором – название файла диска ВМ с расширением, в третьем – периодичность обновления, в четвертом – дата и время последней синхронизации.

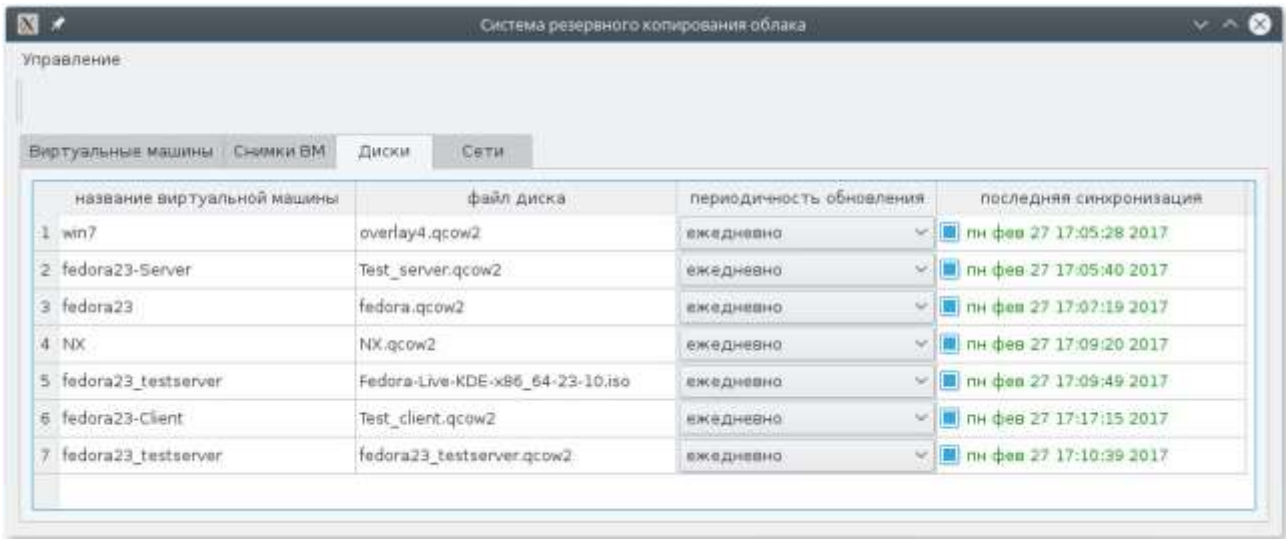


Рисунок 102 - "СРВМ". Диски

На вкладке **Сети** в первом столбце перечислены названия виртуальных сетей, резервные копии конфигураций которых хранятся на сервере резервирования; во втором – периодичность обновления, в третьем – дата и время последней синхронизации.

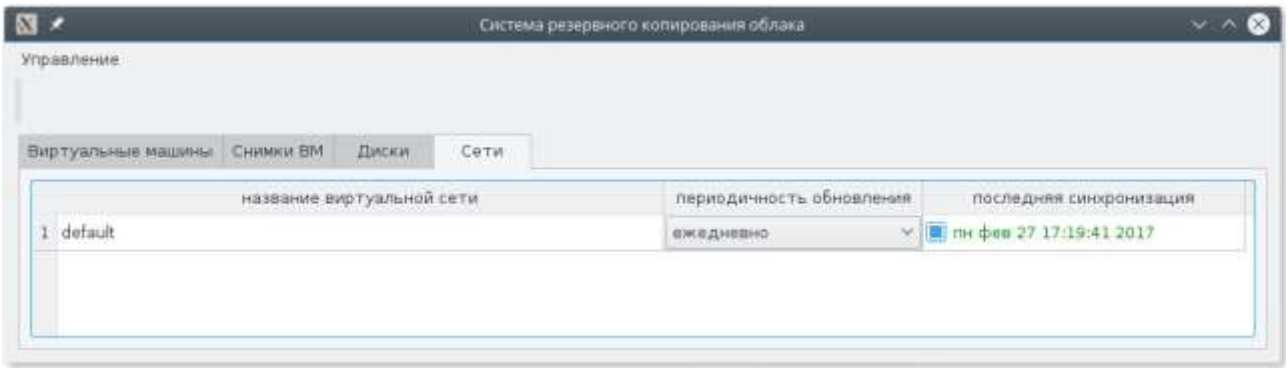


Рисунок 103 - "СРВМ". Сети

Для всех данных периодичность обновления может быть задана администратором: ежедневно, еженедельно и ежемесячно.

Резервные копии сохраняются на сервере резервирования в директории ***/mnt/backup***. Времена сохранения и периодичность обновлений заносятся в файлы в директории ***/var/spool/gbs***.

Для обновления информации о резервных копиях следует зайти в меню *Управление->Загрузить данные* (рисунок 104).

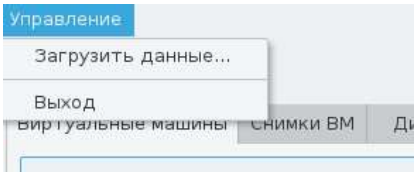


Рисунок 104

Для выхода из графического интерфейса программы “СРВМ” необходимо зайти в меню *Управление->Выход* (рисунок 104).

4 Настройки терминала

4.1 Запуск и настройка терминала

4.1.1 Запуск виртуальной машины на терминале

Перед включением терминала необходимо подключить предварительно подготовленный USB-носитель с установленным программным обеспечением (компонент 1 согласно формуляру МБРЦ.468313.002 ФО) в один из свободных USB-разъемов на терминале. После этого следует включить питание терминала. Далее необходимо зайти в BIOS и установить в качестве основного загрузочного устройства подключенный USB-накопитель.

Примечание. Для того чтобы войти в BIOS, в начале загрузки компьютера необходимо нажать специальную клавишу (например, **Del** или **F2**), когда на экране появится сообщение, предлагающее это сделать. Чаще всего можно встретить сообщения следующего вида: “**Press DEL to enter Setup**”, или “**Press F2 to access the BIOS**”.

4.1.2 Настройка конфигурации терминала

При первой загрузке перед администратором появляется меню с настройками сетевых параметров терминала (рисунок 105). Предоставляется возможность настроить IP адрес, маску подсети, шлюз и DNS сервер.

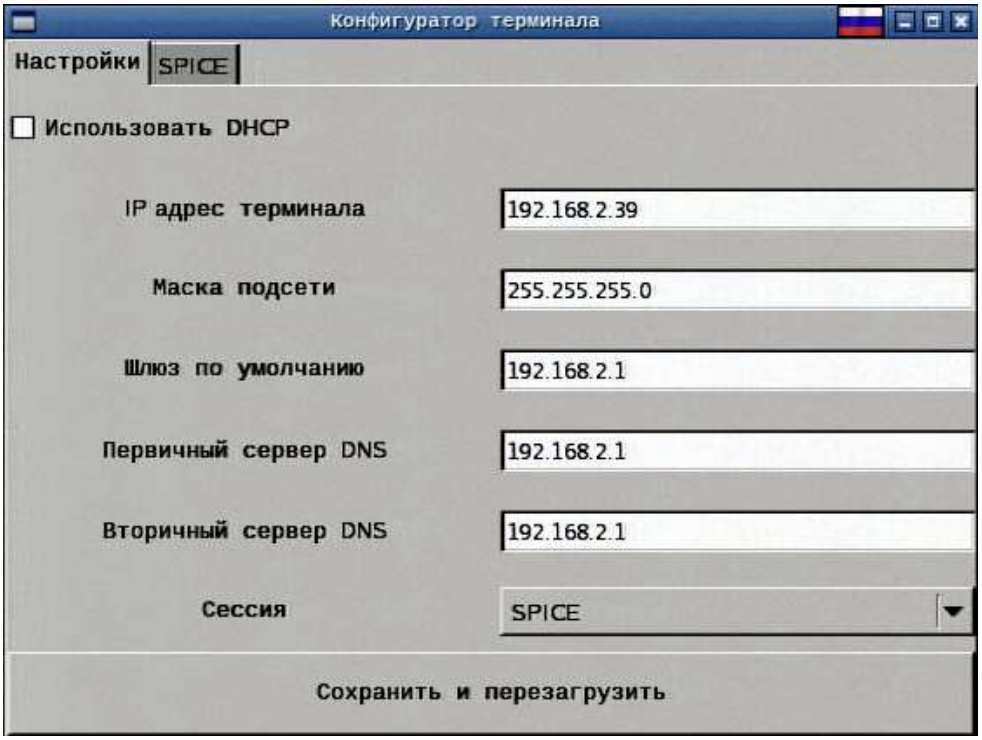


Рисунок 105 – Настройка сетевых параметров терминала

Для настройки протокола SPICE задается адрес сервера и флажками выбираются необходимые опции (рисунок 106).

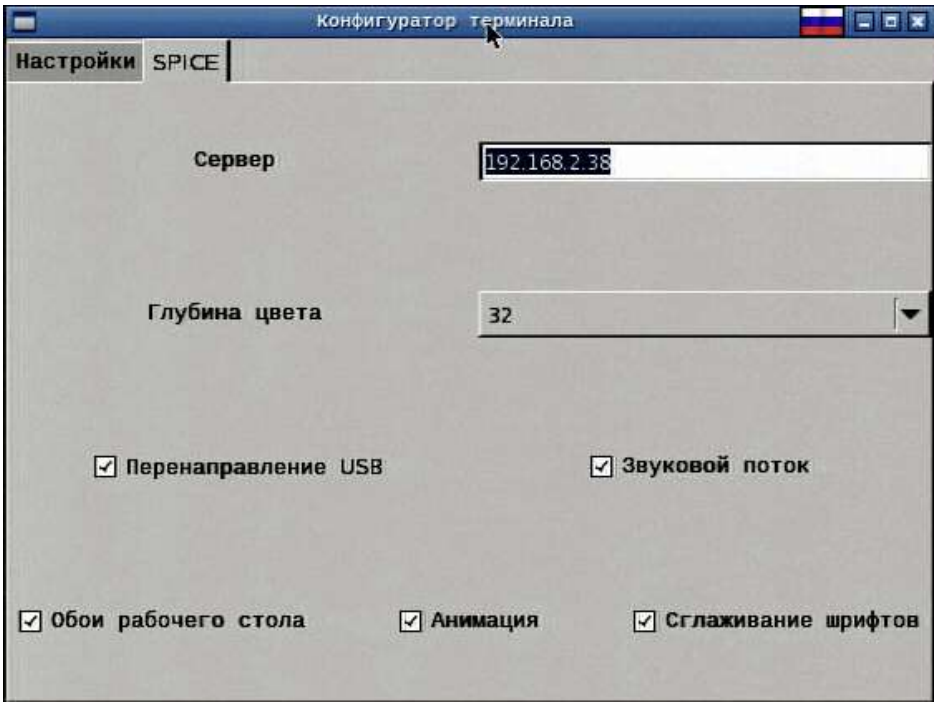


Рисунок 106 – Настройка параметров подключения по протоколу SPICE

ВНИМАНИЕ: *ПО РЕГЛАМЕНТУ КАЖДЫЙ ТЕРМИНАЛ МОЖЕТ БЫТЬ СКОНФИГУРИРОВАН НА ПОДКЛЮЧЕНИЕ ТОЛЬКО К ОДНОМУ СЕРВЕРУ ВИРТУАЛИЗАЦИИ.*

После выполнения всех необходимых настроек следует нажать на кнопку **Сохранить и перезагрузить** на главном экране настроек (рисунок 105). Далее на экран выведется сообщение об успешной настройке терминала. Следует нажать кнопку **ОК**, и компьютер будет перезагружен.

Для того чтобы настроить *терминал* на подключение к другому *серверу виртуализации*, необходимо подключить USB-носитель к *серверу виртуализации* и удалить конфигурационный файл ***vsc.conf***. После установки USB-носителя на *терминале* вновь появится меню с настройками параметров (рисунок 105).

4.2 Подключение принтера

Для подключения ВМ к серверу печати в ОС Windows 7 необходимо зайти в меню *«Пуск»->»Устройства и принтеры»*. В открывшемся окне следует нажать кнопку **Установка принтера** (рисунок 107).

Рисунок 107 – Устройства и принтеры

В следующем окне нужно выбрать пункт **Добавить сетевой, беспроводной или Bluetooth- принтер** и нажать кнопку **Далее**.

Если принтер не был найден автоматически, то следует нажать на указатель **Нужный принтер отсутствует в списке** (рисунок 108).

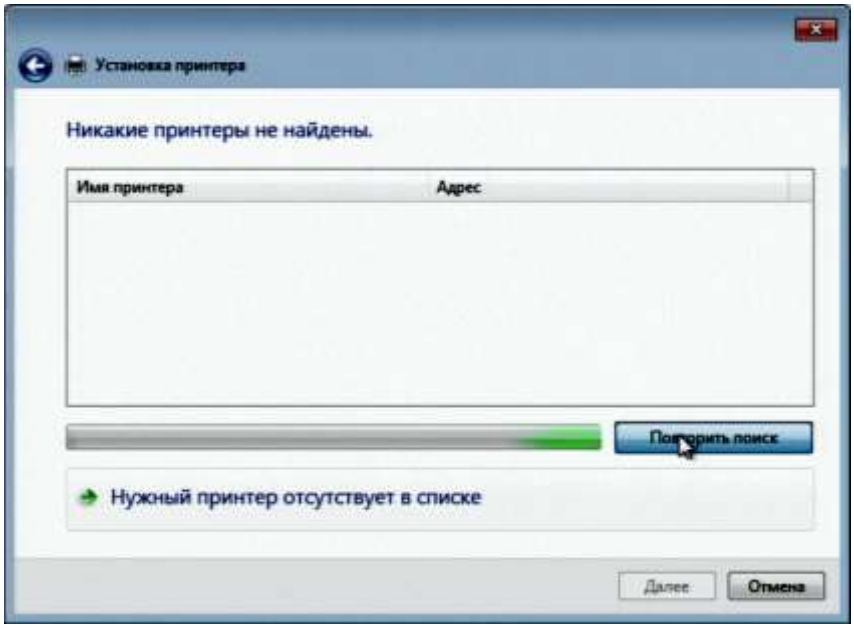


Рисунок 108 – Установка принтера

После этого выбрать пункт **Добавить принтер по его TCP/IP-адресу или имени узла** и нажать **Далее**. В следующем окне (рисунок 109) выбрать из ниспадающего списка тип устройства – **Устройство TCP/IP**, ввести IP-адрес и имя порта и нажать кнопку **Далее**.

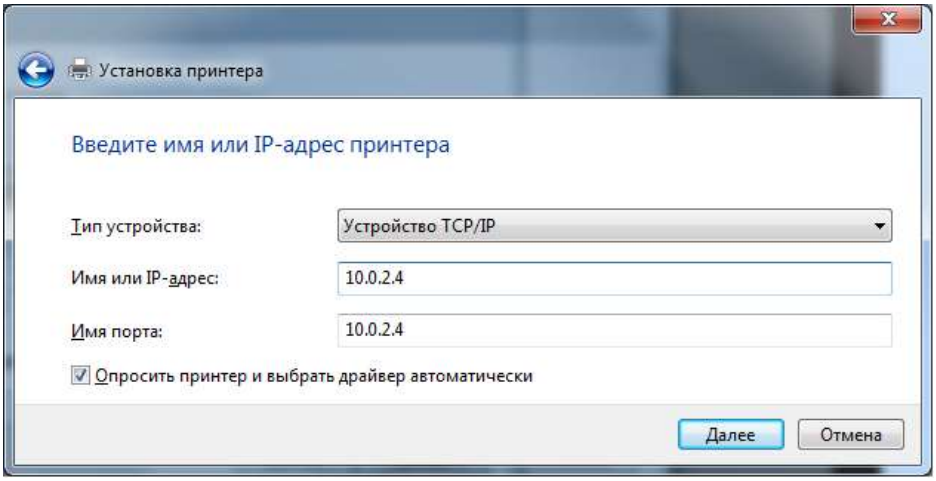


Рисунок 109 – Ввод имени и IP-адреса принтера

При печати документа из гостевой операционной системы, определяется мандатная метка виртуального окружения, и в соответствии с этой меткой, средствами сервера виртуализации в документ могут быть добавлены дополнительные специальные атрибуты («фонарик», атрибуты пользователя и т.д.).

После подачи любого файла на печать на экране монитора *терминала* появляется окно, в которое требуется ввести данные о распечатываемом документе и операторе. Подробнее работа описана в документе “ПИ “Горизонт-ВС”. Руководство по эксплуатации” МБРЦ.468313.002 РЭ.

5 Настройка системы группового управления

5.1 Общие сведения

Система группового управления (СГУ) ПИ “Горизонт-ВС” предназначена для удаленного создания и управления виртуальной инфраструктурой на базе универсальных серверных платформ x86-64 с применением аппаратной виртуализации.

Добавление вычислительных узлов в кластер и их удаление обеспечивается без необходимости первоначальной настройки виртуальной инфраструктуры. В момент добавления нового узла в кластер обеспечивается его автоматическая настройка.

СГУ позволяет управлять полным жизненным циклом виртуальных машин с возможностью их клонирования и миграции.

5.2 Вход в СГУ

Для подключения к СГУ следует ввести в адресной строке браузера IP-адрес узла АРМ УВ (например, *https://192.168.2.40*). В открывшемся окне аутентификации ввести имя пользователя и пароль (рисунок 110).

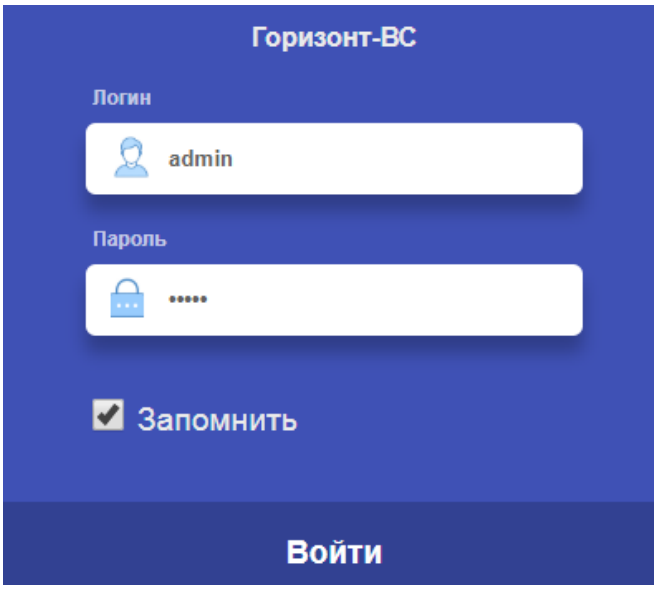


Рисунок 110 – Окно аутентификации

Примечание. По умолчанию имя пользователя и пароль «*admin/admin*». Изменить пароль администратора можно в разделе «*Система*»-«*Пользователи*».

После успешной аутентификации будет получен доступ к главному окну СГУ – **Информационная панель** (рисунок 111).

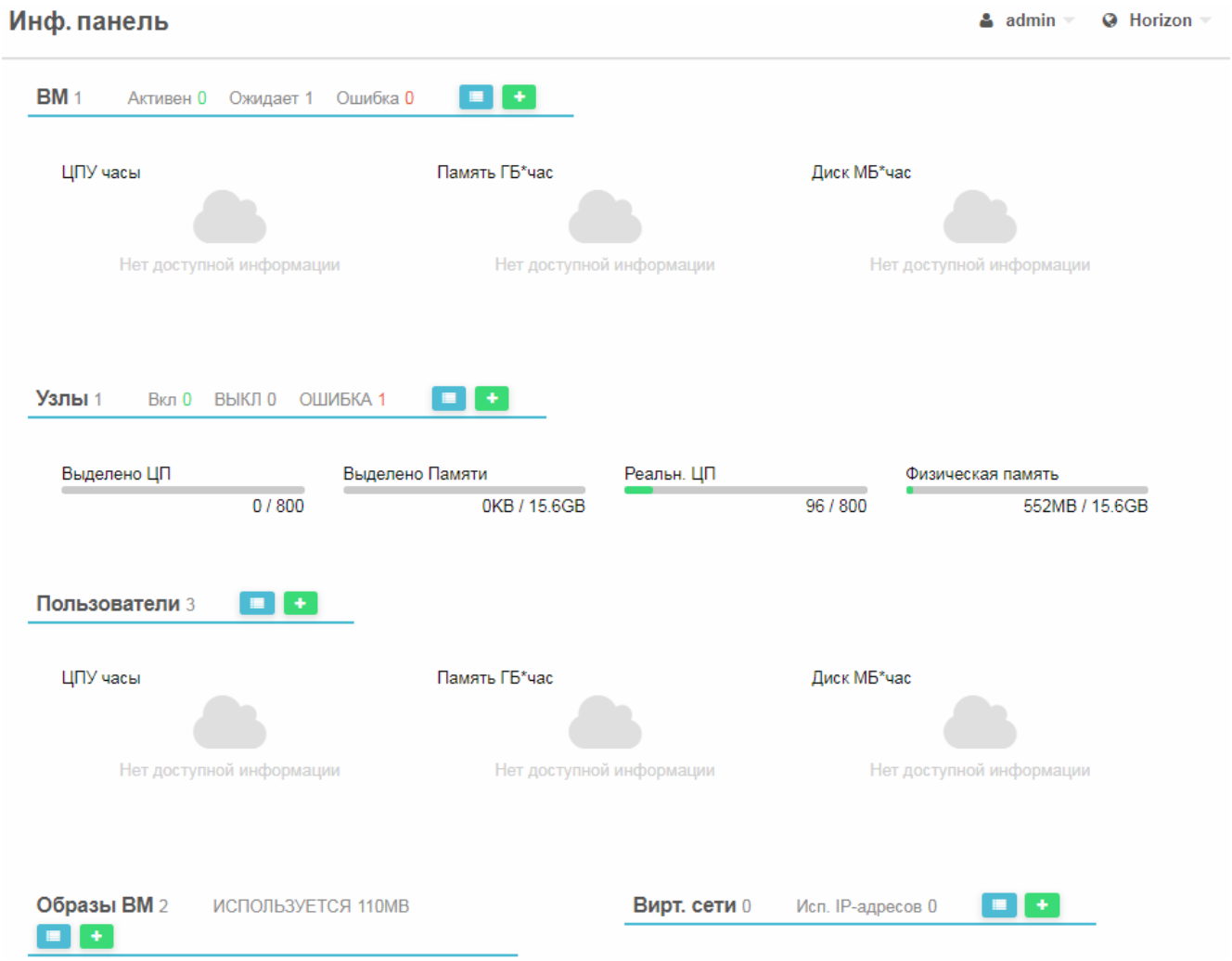


Рисунок 111 – Веб-интерфейс СГУ

В левой колонке размещено меню управления системой. В верхней части – навигация, имя пользователя и наименование ведущей хостинговой зоны (зоны управления).

Раздел **ВМ** содержит информацию о количестве:

- созданных ВМ;
- функционирующих (активных) ВМ;
- размещаемых в данный момент времени ВМ в системе (режим ожидания);
- сообщения об ошибках.

На диаграммах представлены сведения о загрузке ЦПУ, оперативной памяти и дискового пространства как по всем ВМ, размещенных в системе, так и по каждой ВМ в отдельности (рисунок 112).

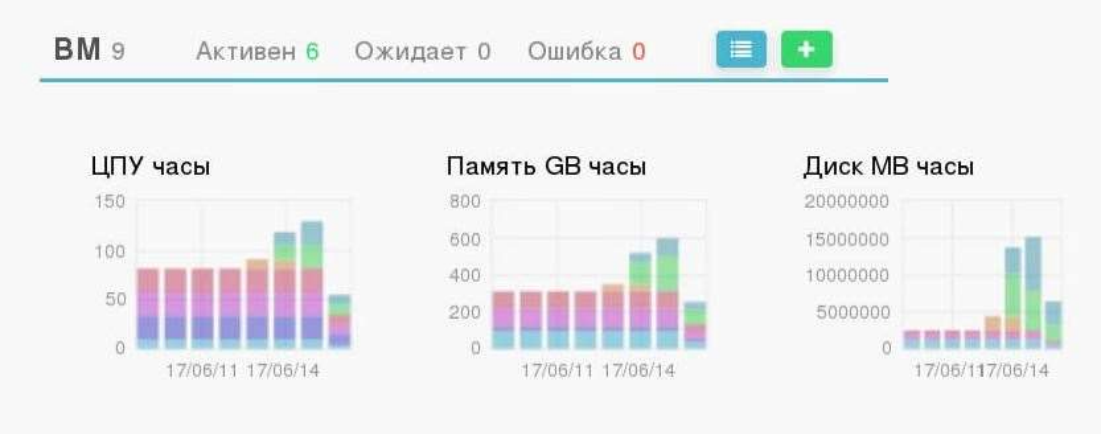


Рисунок 112 – Сведения о ВМ

Раздел **Узлы** содержит следующую информацию:

- количество физических серверных узлов, зарегистрированных в системе;
- количество функционирующих и отключенных узлов;
- количество сообщений об ошибках.

Мониторинг суммарного использования (рисунок 113):

- совокупной процессорной мощности в системе;
- мониторинг использования выделенных ресурсов ЦП для ВМ;
- суммарный и используемый объем оперативной памяти в системе.

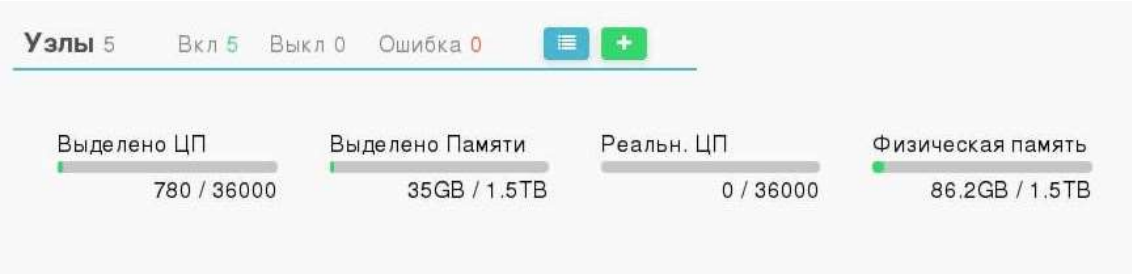


Рисунок 113 – Мониторинг узлов системы

Раздел **Пользователи** содержит информацию о количестве зарегистрированных пользователей и администраторов в системе. На рисунке 114 представлен мониторинг суммарного использования ресурсов (ЦПУ, пространства в СХД, оперативной памяти) каждым пользователем.

Рисунок 114 – Мониторинг пользователей

Раздел **Образы ВМ** содержит информацию о количестве созданных образов в зоне управления и используемый объем диска или подключенного хранилища (рисунок 115).

Раздел **Виртуальные сети** содержит информацию о количестве созданных виртуальных сетей и используемых в зоне управления IP-адресов (рисунок 115).

Рисунок 115 – Образы ВМ и Виртуальные сети

В каждом разделе с помощью кнопки предусмотрен переход на соответствующую страницу СГУ:

- экземпляры ВМ/ВМ;
- инфраструктура/узлы;
- система/пользователи;
- хранилище/образы ВМ;
- сеть/виртуальные сети.

С помощью кнопки  осуществляется переход на страницу создания либо регистрации нового ресурса (узла, ВМ, виртуальной сети, хранилища, пользователя и т.д.).

5.3 Создание зон управления

Зона управления – это логическое объединение серверов виртуализации в группы по функциональному или иному признаку. После установки СГУ в системе по умолчанию регистрируется ведущая зона управления с конечной точкой ***http://адрес ядра системы группового управления зоной:2633/RPC2***. Ее параметры отображены в разделе **Инфраструктура** подразделе **Зоны** (рисунок 116).

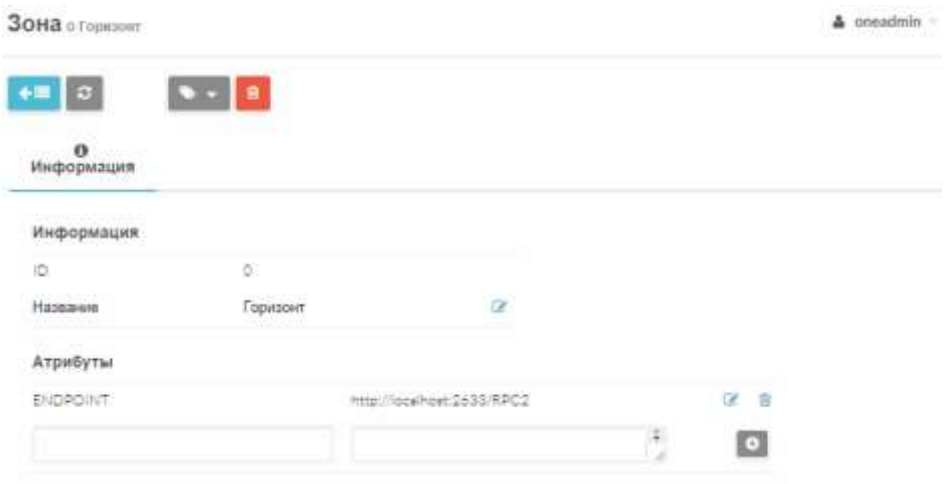


Рисунок 116 - Зона управления

Атрибутами зоны являются ссылки на сервера виртуализации. В пределах зоны ограничена видимость следующих ресурсов из других зон:

- экземпляры ВМ;
- узлы;
- пользователи;
- образы ВМ;
- виртуальные сети.

5.4 Регистрация узла

Для подключения к СГУ и регистрации в зоне управления серверов виртуализации (узлов) с установленными на них ПИ “Горизонт-ВС” необходимо зайти в раздел *«Инфраструктура»–>«Узлы»* и нажать кнопку  - на экране появится окно регистрации нового узла (рисунок 117).

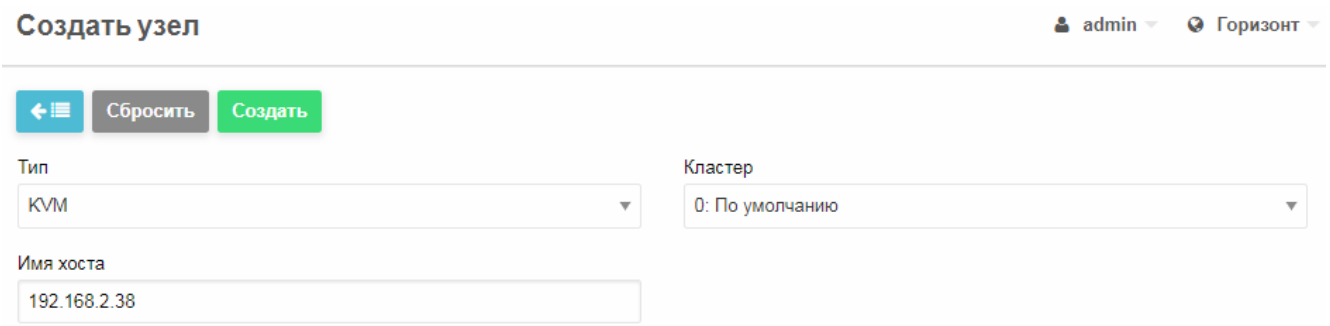


Рисунок 117 – Создание узла

В поле **Тип** выбирается модуль ядра поддержки виртуализации (значение по умолчанию – KVM). В поле **Кластер** выбирается наименование кластера, к которому будет подключаться новый узел (в первоначальных настройках системы создается кластер “0: По умолчанию”). В поле **Имя хоста** вводится IP-адрес подключаемого узла. После заполнения всех данных необходимо нажать кнопку **Создать**, после чего начнется процесс инициализации нового узла в зоне управления и размещение его в выбранном кластере.

Примечание. Необходимо зарегистрировать в СГУ узел АРМ УВ.

5.5 Организация кластеров

Раздел СГУ *«Инфраструктура»–>»Кластеры»* позволяет создать необходимое количество кластеров и распределить между ними зарегистрированные в системе узлы, в зависимости от исполняемых на них задач и их функционального назначения (рисунок 118).

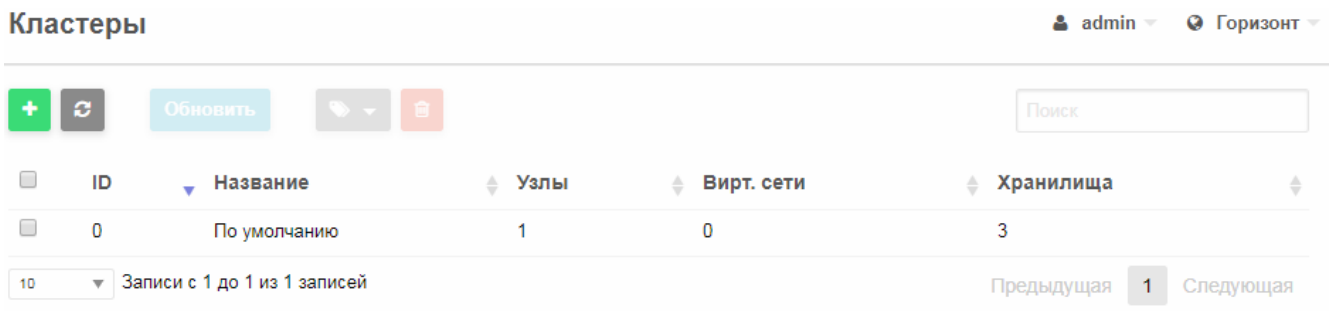


Рисунок 118 – Раздел «Кластеры»

Для создания кластера следует нажать кнопку «**+**» (рисунок 118) В открывшемся окне ввести имя кластера в поле **Название**, выбрать не менее двух узлов из списка и нажать кнопку **Создать** (рисунок 119);

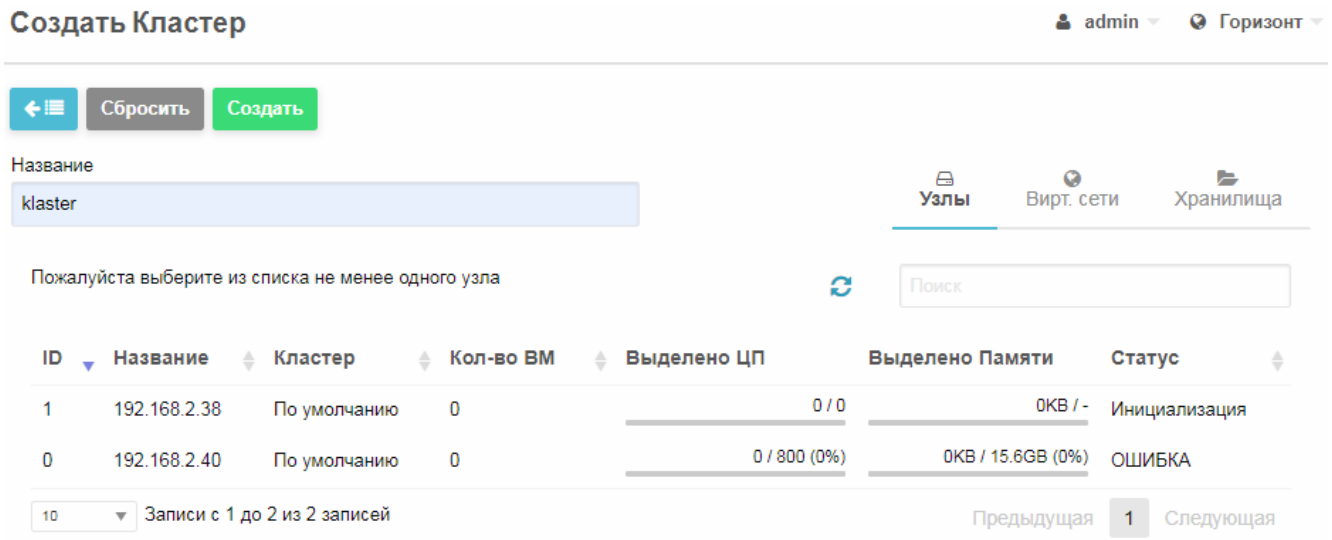


Рисунок 119

Для изменения конфигурации кластера необходимо выделить его флажком в таблице (см. рисунок 118) и нажать активизировавшуюся кнопку **Обновить**. В открывшемся окне во вкладке **Узлы** появляется возможность отсоединить или подключить дополнительные хосты, во вкладке **Виртуальные сети** изменить наличие и количество используемых виртуальных сетей, во вкладке **Хранилища** выбрать используемые этим кластером хранилища (рисунок 120).

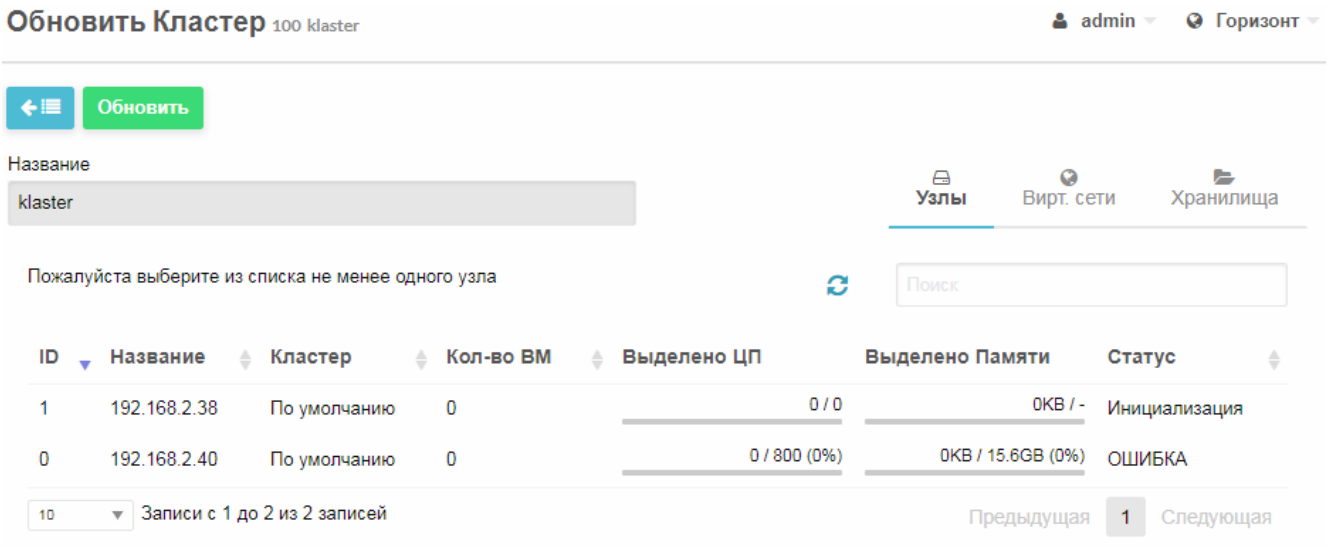


Рисунок 120 – Обновление кластеров

5.6 Создание хранилища

Для создания хранилища следует зайти в СГУ *“Хранилище”→“Хранилища”*, после чего откроется окно, в котором в виде списка представлены хранилища, уже существующие в системе (рисунок 121).

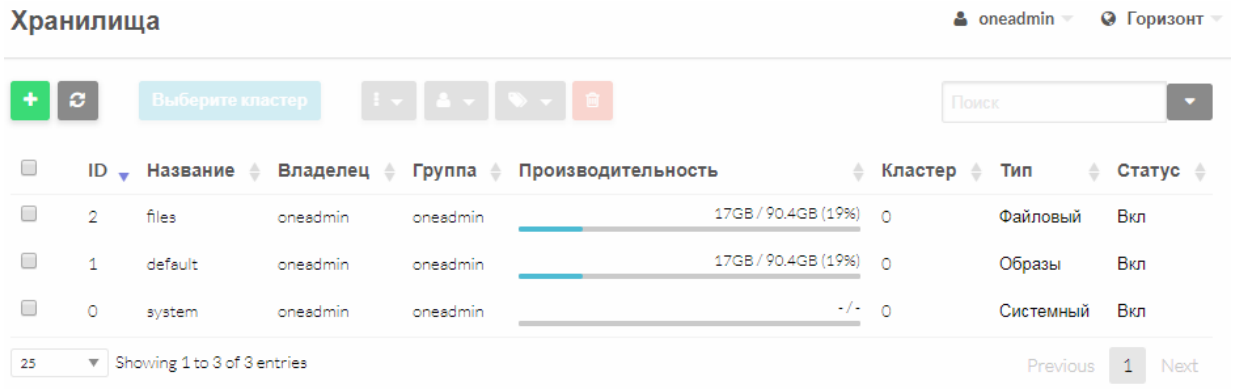


Рисунок 121 – Менеджер хранилищ

Для создания нового хранилища необходимо нажать кнопку “+” в управляющем меню – откроется окно **Создать хранилище** (рисунок 122).

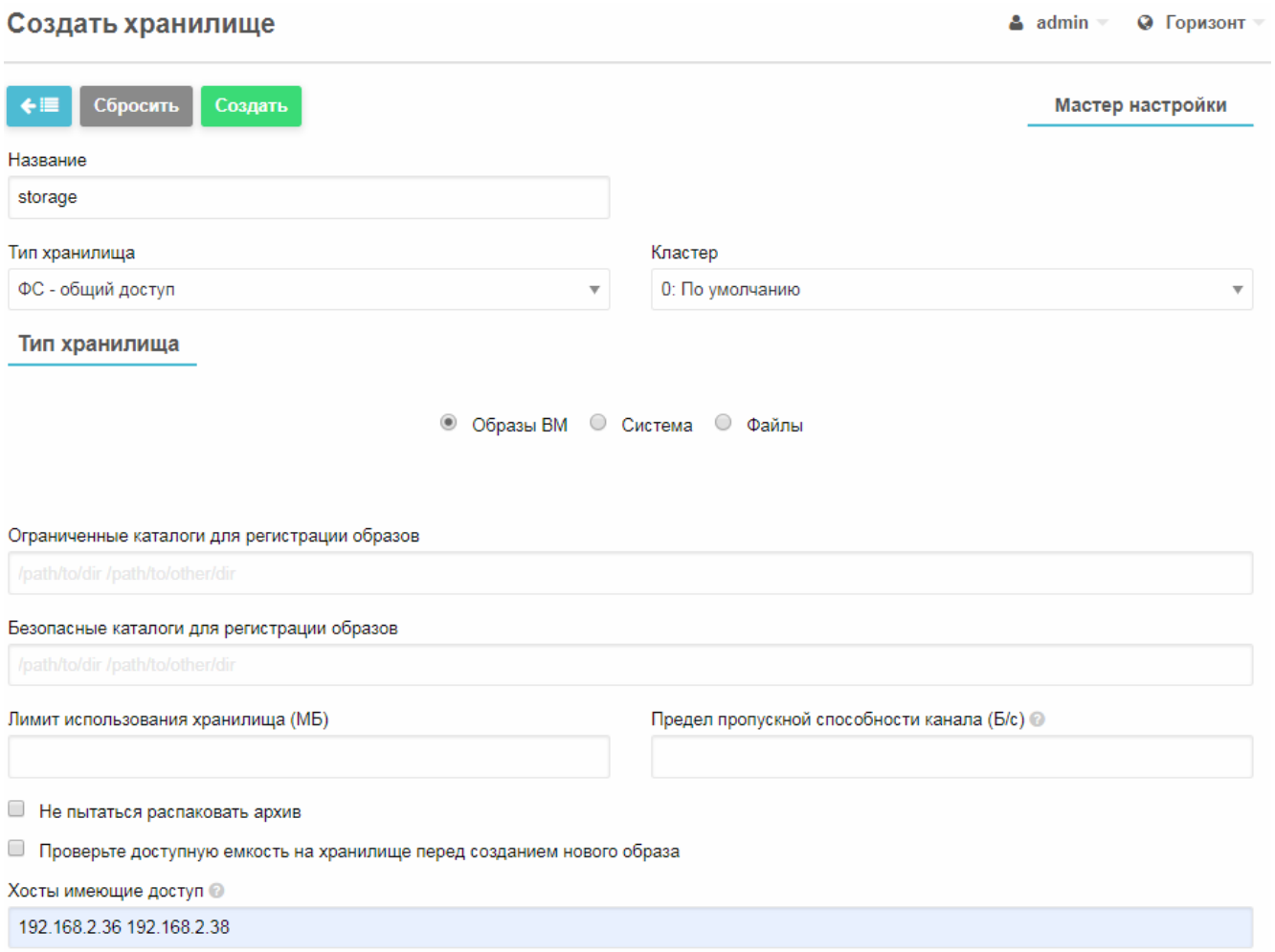


Рисунок 122 – Создание хранилища

В открывшемся окне необходимо ввести название хранилища, кластер, на котором оно будет расположено, из раскрывающегося списка **Тип хранилища** выбрать протокол хранилища (рисунок 123).

Рисунок 123 – Протоколы для хранилища

При помощи переключателей возможно установить тип хранилища: “**Образы *ВМ***”, “**Система**”, “**Файлы**”.

Тип “**Образы ВМ**” предназначен для хранения образов ВМ, образов жестких дисков, образов установочных дисков с ОС и другого ПО.

Тип “**Система**” предназначен для хранения файлов самой СГУ.

Тип “**Файлы**” предназначен для хранения простых файлов (не образов), которые могут быть использованы в качестве виртуальных ядер, RAM-дисков, загрузочных дисков, файлов контекста.

Возможно заполнить поля “**Хосты имеющие доступ**” для указания адресов серверов виртуализации, которые будут иметь доступ к данному хранилищу, и указать лимит использования хранилища в МБ.

После заполнения всех необходимых полей следует нажать кнопку **Создать**, и новое хранилище появится в списке.

5.7 Создание установочного образа диска виртуальной машины

Образ установочного диска виртуальной машины необходим для создания ВМ.

Для создания установочного образа диска гостевой ОС необходимо в разделе **Хранилище** выбрать подраздел **Образ ВМ** и нажать кнопку  , после чего откроется окно (рисунок 124).

В поле “**Название**” указывается наименование образа диска. В поле **Тип** из раскрывающегося списка выбирается “**Образ операционной системы**”. В поле **Хранилище** указывается тип хранилища, в котором будет храниться образ. В поле **Описание** для удобства использования СГУ вносится дополнительная информация о содержащейся на образе ОС.

Затем в разделе страницы **Расположение образа** следует установить переключатель **Закачать**, с помощью кнопки **Выберите файл** выбрать необходимый iso-образ установочного диска.

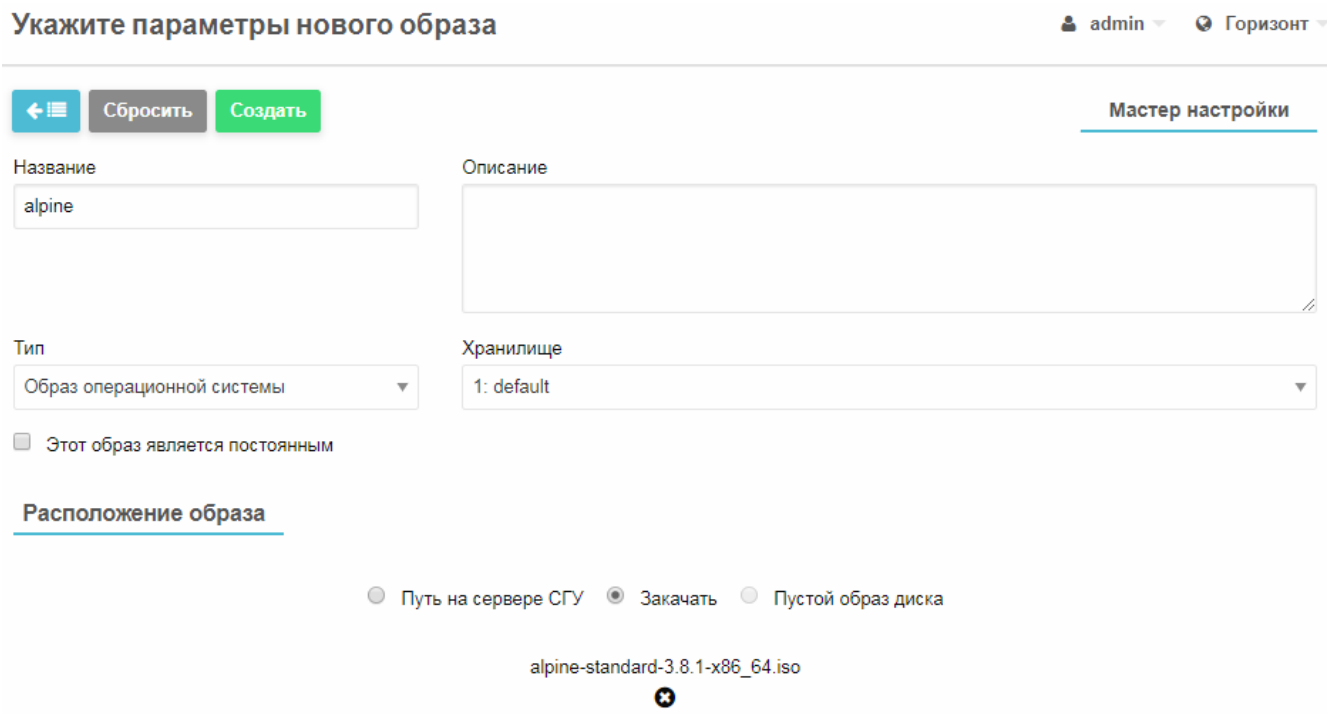


Рисунок 124 – Создание установочного образа диска ВМ

Когда все необходимые поля будут заполнены, следует нажать кнопку **Создать**. После завершения процесса копирования iso-файла образ жесткого диска с данными будет создан и размещен в хранилище.

5.8 Создание дисковых разделов

Для создания в хранилище дисковых разделов, которые будут использованы для создания гостевой ОС и хранения данных, необходимо в разделе **Хранилище** выбрать подраздел **Образы ВМ** и нажать кнопку  .

В открывшемся окне (рисунок 125) в поле **Название** ввести наименование диска.

В поле **Тип** из раскрывающегося списка выбрать подпункт **Блок данных**.

В поле **Хранилище** указать хранилище, где будет храниться образ.

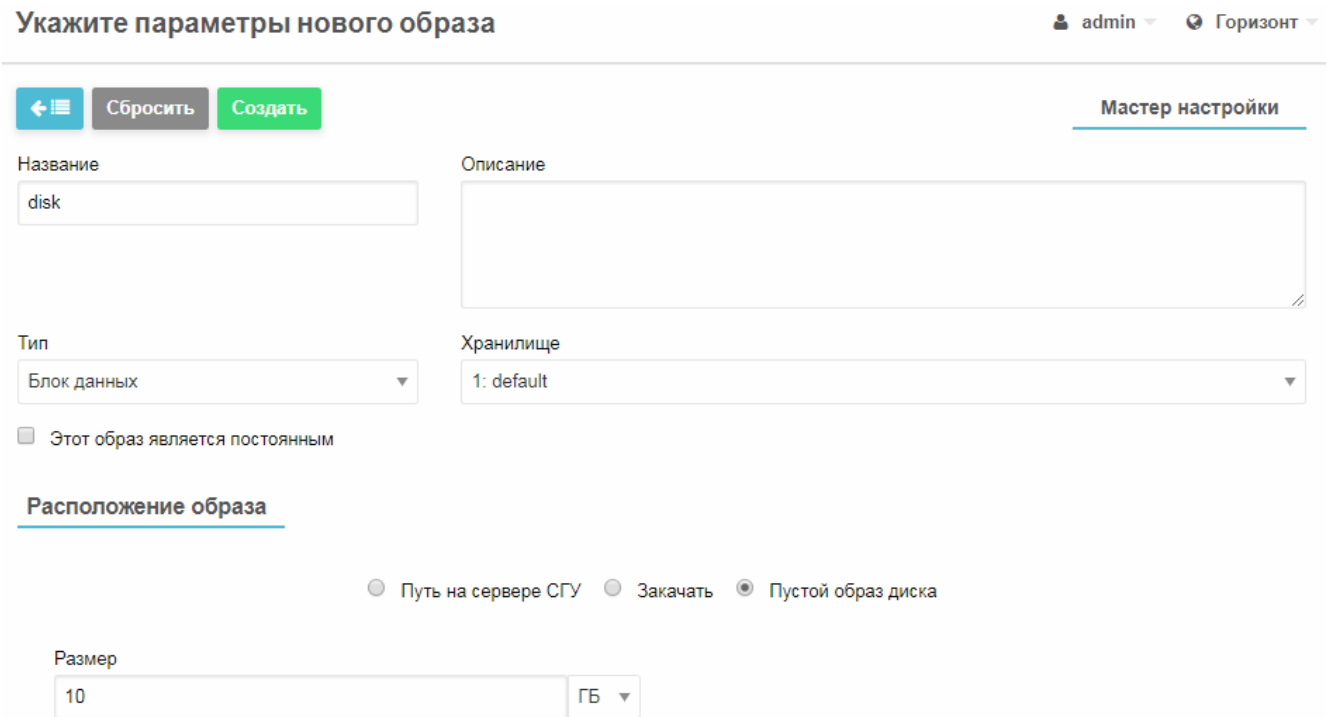


Рисунок 125 – Создание шаблона жесткого диска

В поле **Описание** можно ввести дополнительную информацию о диске: параметры образа, функциональное предназначение и т.д.

Затем в разделе **Расположение образа** установить переключатель **Пустой образ диска** и в появившемся поле указать размер виртуального жесткого диска ВМ в МБ или ГБ.

Примечание: если предполагается осуществлять миграцию виртуального диска, следует установить флажок «Этот образ является постоянным»

После этого нажать кнопку **Создать** и дождаться размещения образа ВМ в хранилище.

5.9 Загрузка образов ОС в хранилище

Для создания ВМ необходимо разместить в хранилище образов виртуальных дисков, установочный образ дистрибутив ОС.

Для размещения образа ОС необходимо в разделе **Хранилище** выбрать подраздел **Образ ВМ** и нажать кнопку  .

В открывшемся окне (рисунок 126) в поле **Название** ввести наименование образа ОС. В поле **Тип** из раскрывающегося списка выбрать пункт **CD-ROM только для чтения**. В поле **Хранилище** указать тип хранилища, где будет храниться образ. В поле **Описание** для удобства работы с СГУ ввести дополнительную информацию о содержащейся на образе ОС.

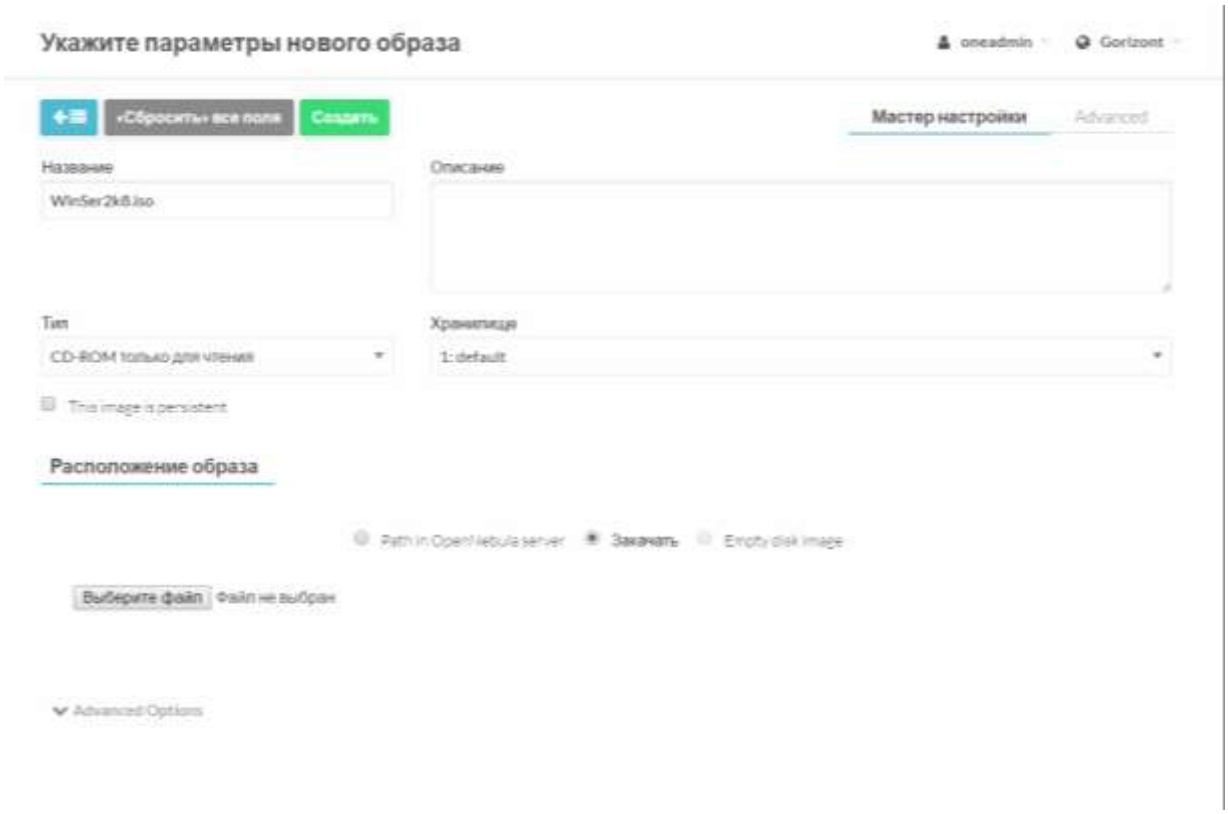


Рисунок 126 – Создание образа ВМ с CD-ROM

В разделе страницы **Расположение образа** установить переключатель **Закачать**, с помощью кнопки **Выберите файл** выбрать необходимый iso-образ установочного диска с ОС и нажать кнопку **Создать**.

После завершения процесса копирования iso-образа виртуальный CD-ROM с установочным диском гостевой ОС будет создан и размещен в хранилище.

5.10 Создание и удаление пользователей

Для работы с пользователями виртуальных машин следует зайти в СГУ *Система→Пользователи*, после чего откроется окно (рисунок 127).

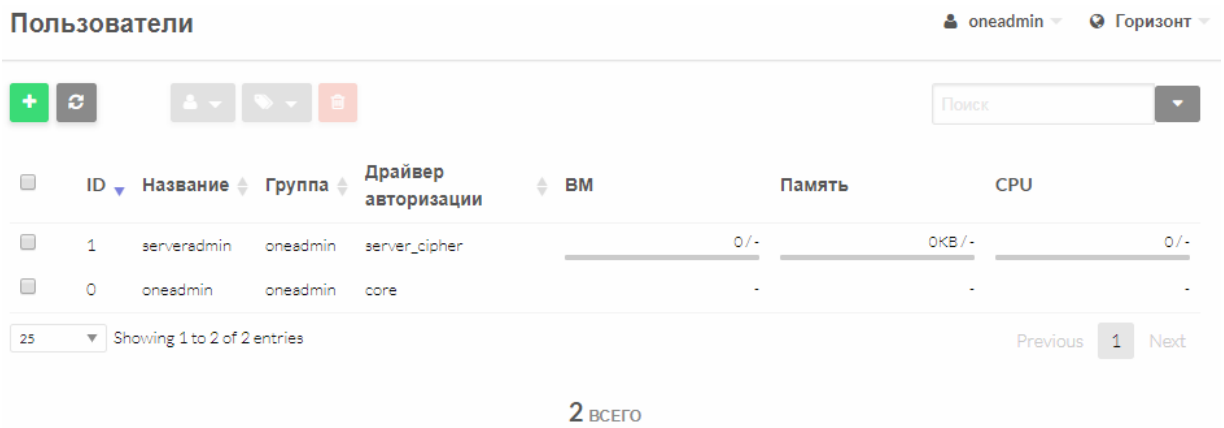


Рисунок 127 – Менеджер пользователей ВМ

Для создания нового пользователя необходимо нажать кнопку «+» в управляющем меню – откроется окно **Создать пользователя** (рисунок 128).

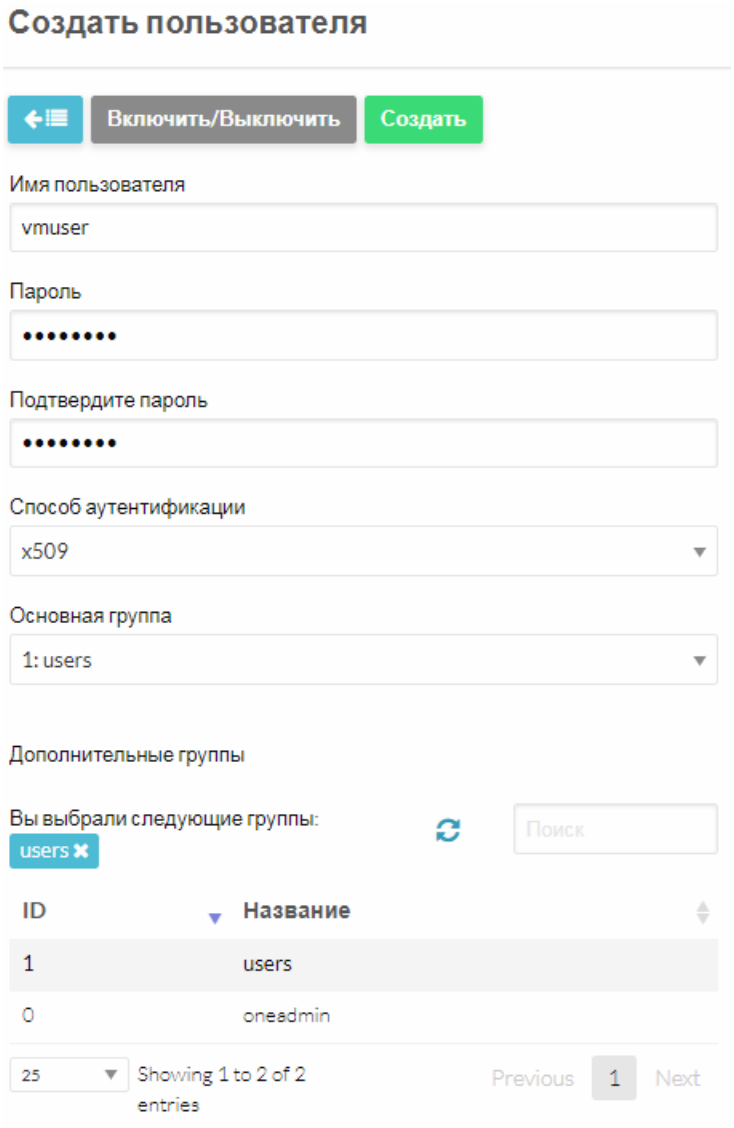


Рисунок 128 – Новый пользователь ВМ

В открывшемся окне следует ввести следующие данные:

– **имя пользователя** – имя пользователя, как оно будет отображаться в системе;

– **пароль** и **подтвердить пароль** – пароль пользователя;

– из раскрывающегося списка выбрать способ аутентификации;

– выбрать основную группу, в которую будет входить пользователь.

После заполнения всех полей нужно нажать кнопку **Создать** (рисунок 128), и в главном окне (рисунок 127) в списке появится новый пользователь.

Примечания:

1. Если не все поля будут заполнены, то на экране появится предупреждающее сообщение (рис. 129).

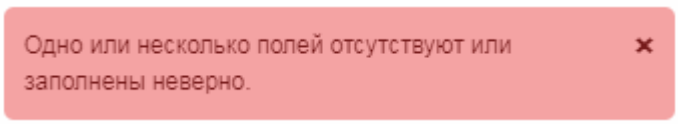


Рисунок 129 – Сообщение

2. Имя пользователя должно быть уникальным. Если будет введено имя, уже существующее в системе, то на экране появится предупреждающее сообщение (рис. 130).

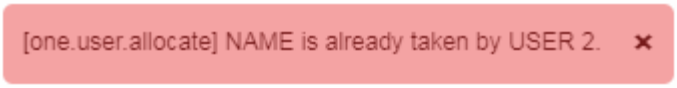


Рисунок 130 – Сообщение

Для удаления пользователя необходимо выделить в списке (рисунок 127) нужного пользователя и нажать кнопку  в управляющем меню – появится предупреждающее сообщение (рисунок 131).

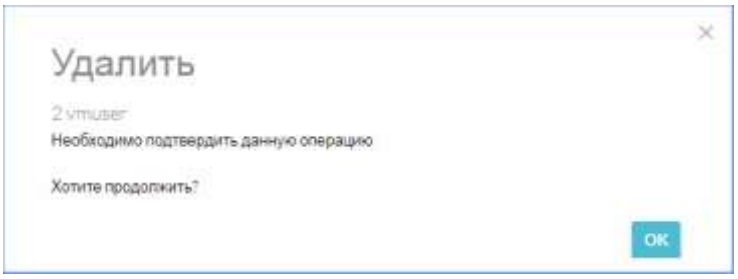


Рисунок 131 – Предупреждающее сообщение

Для подтверждения удаления следует нажать кнопку **ОК**, после чего пользователь будет удален.

5.11 Создание групп пользователей

Для разграничения прав в ПИ “Горизонт-ВС”, помимо пользователей, существуют группы. Также, как и пользователь, группа обладает правам доступа к тем или иным каталогам, файлам, ВМ и т.д. Для каждого ресурса определён не только пользователь, но и группа. Группы группируют пользователей для предоставления одинаковых полномочий на какие-либо действия.

Принадлежность пользователя к группе устанавливается администратором.

Для работы с пользователями виртуальных машин следует зайти в СГУ *Система→Группы*, после чего на экране откроется список зарегистрированных в системе групп (рисунок 132).

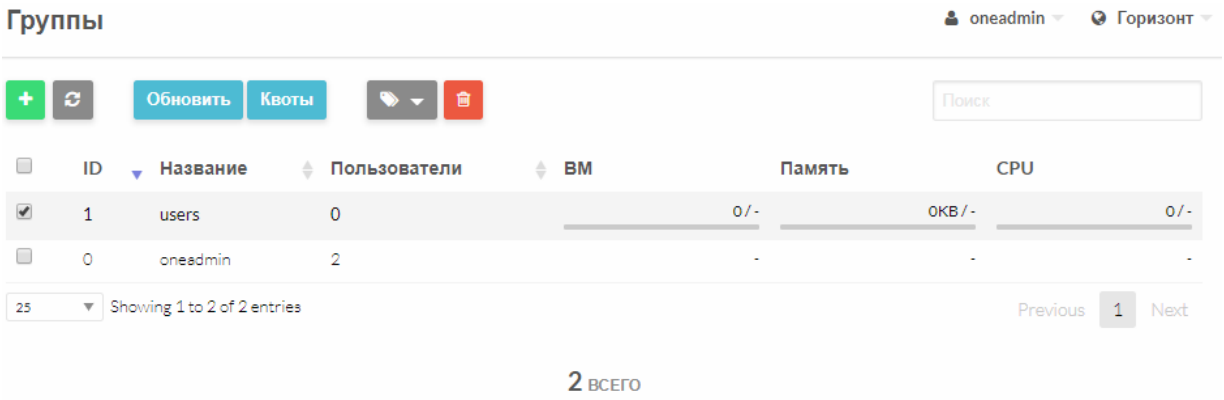


Рисунок 132 – Группы пользователей

Для создания новой группы необходимо нажать кнопку “+”, после чего на экране откроется окно **Создать группу** на вкладке **Общие** (рисунок 133).

В поле **Название** следует ввести имя группы, как оно будет отображаться в системе.

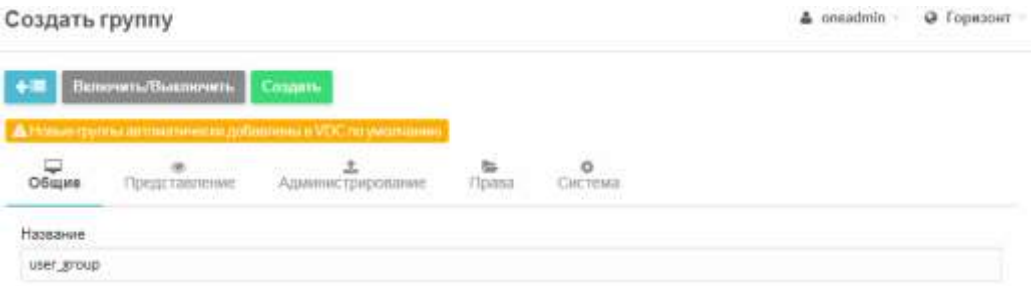


Рисунок 133 – Создание группы. Вкладка "Общие"

На вкладке **Представление** необходимо указать стандартный пользовательский и административный интерфейсы, а также установить флажками представление группы в качестве группы пользователей или администраторов (рисунок 134).

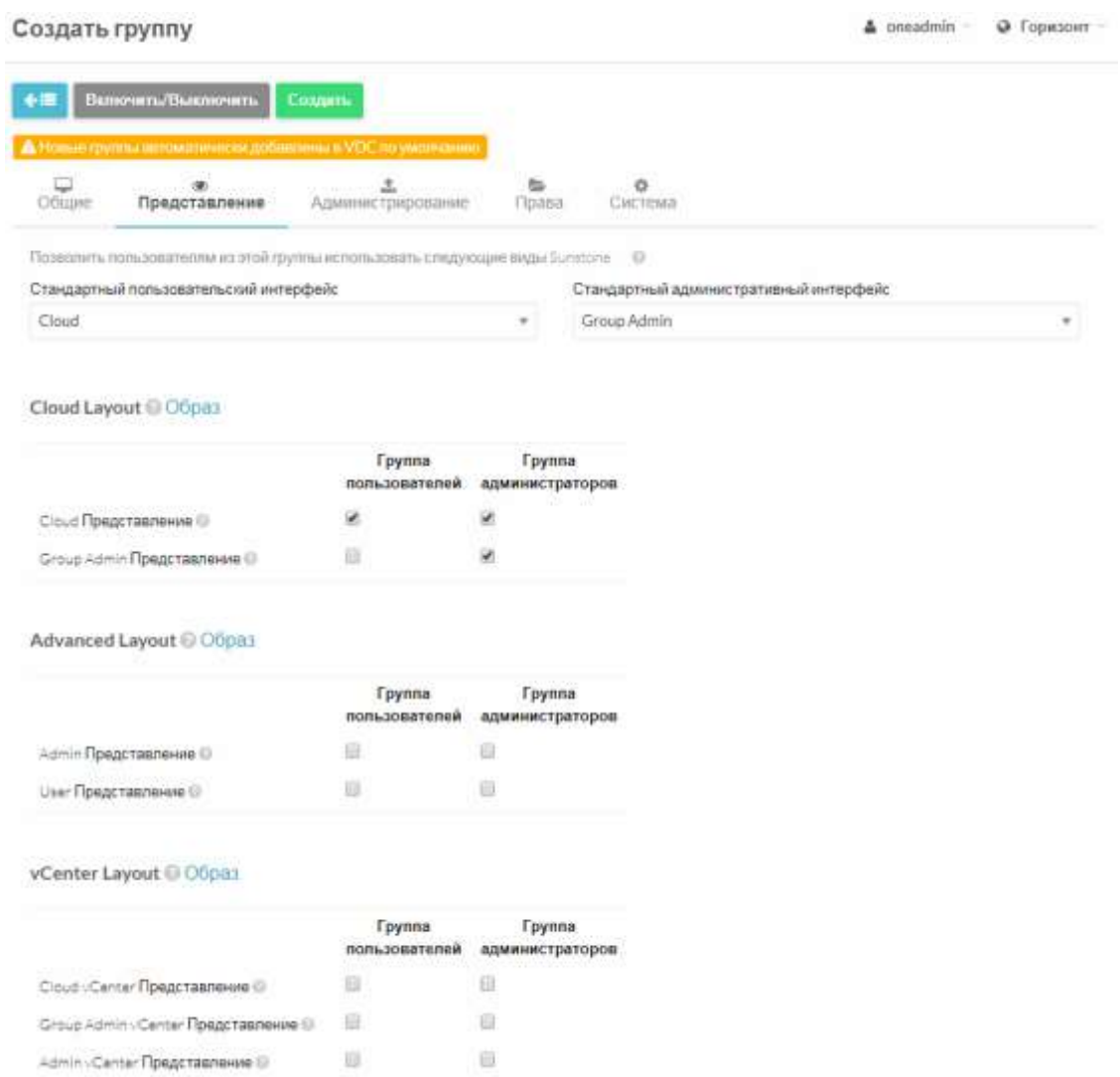


Рисунок 134 – Создание группы. Вкладка "Представление"

На вкладке **Администрирование** предоставляется возможность создать пользователя группы с административными правами. Для этого следует установить соответствующий флажок, после чего станут активными поля **Имя пользователя**, **Пароль**, **Подтвердите пароль** и **Способ аутентификации**, которые необходимо заполнить (рисунок 135).

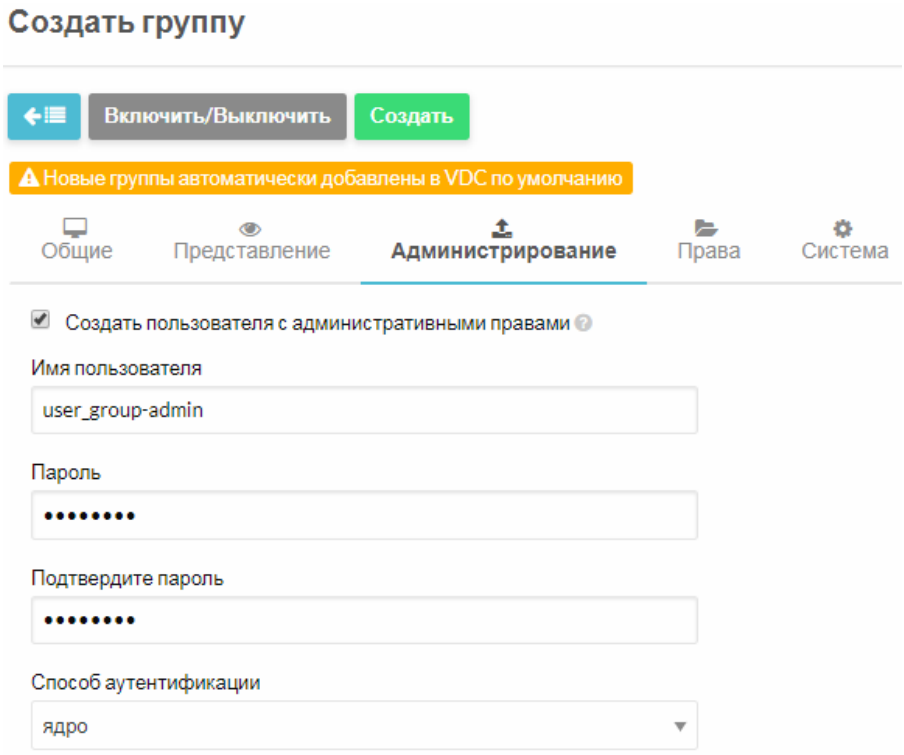


Рисунок 135 – Создание группы. Вкладка "Администрирование"

На вкладке **Права** устанавливаются разрешения на создание ресурсов для пользователей группы (рисунок 136). Разрешенные ресурсы отмечаются флажками.

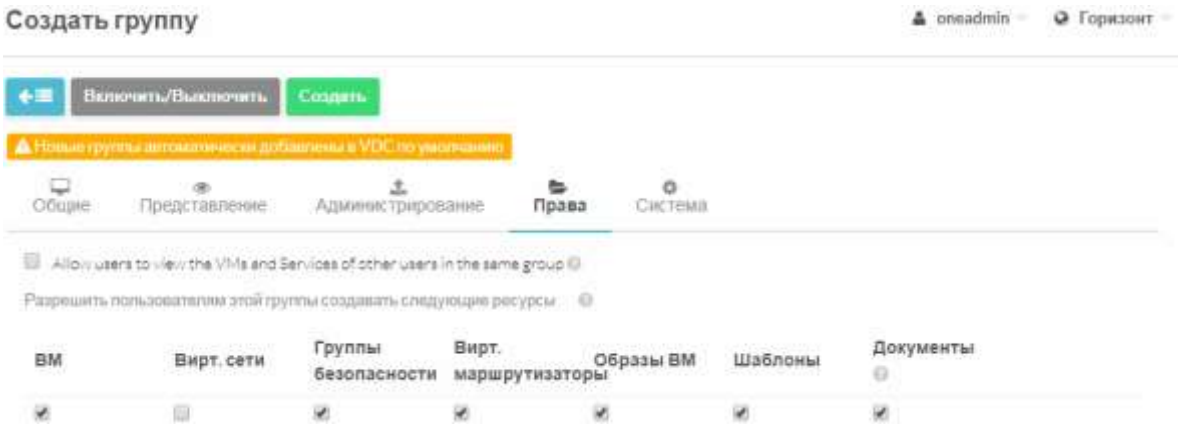


Рисунок 136 – Создание группы. Вкладка "Права"

После заполнения необходимых полей на вкладках следует нажать кнопку **Создать**, новая группа появится в списке (рисунок 132).

5.12 Создание и настройка виртуальных сетей

Для того чтобы создать новую сеть, нужно перейти в раздел СГУ *Сеть→Виртуальные сети* и нажать кнопку “+”, после чего запустится процесс создания сети, в ходе которого необходимо заполнить несколько вкладок.

На вкладке **Общие** необходимо ввести имя сети в поле **Название** и описание (рисунок 137).

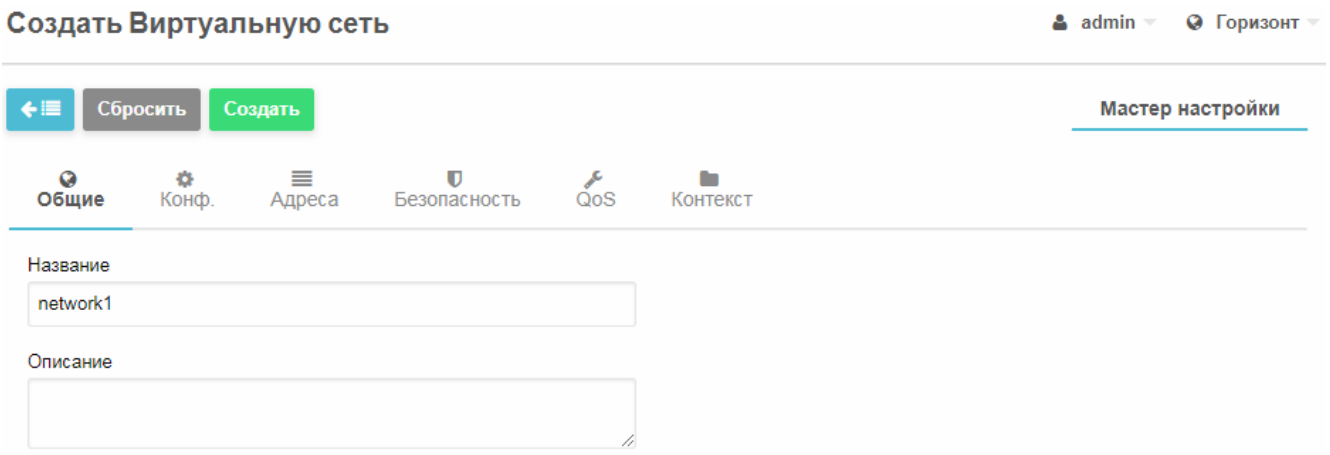


Рисунок 137 – Создание виртуальной сети. Вкладка «Общие»

На вкладке **Конф.** следует в поле **Интерфейс сет. моста** ввести название физического интерфейса, созданного в разделе 3.3 (рисунок 138).

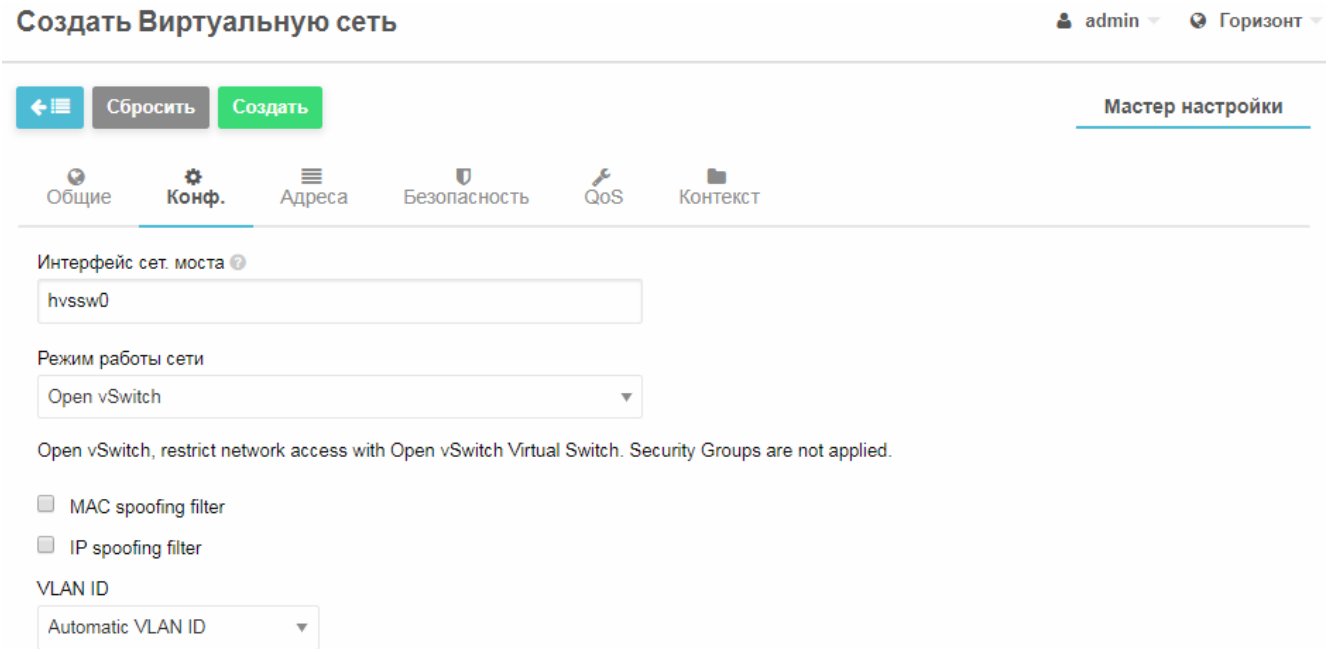


Рисунок 138 – Создание новой виртуальной сети. Вкладка «Конф.»

Из раскрывающегося списка следует выбрать режим работы сети (рисунок 139).

Рисунок 139 – Режимы работы виртуальной сети

Режим работы **Bridged** – сетевой мост, режим работы **802.1Q** – VLAN, режим работы **VXLAN** – для поддержки OpenFlow.

На вкладке **Адреса** нужно при помощи переключателей установить протокол сети (IPv4, IPv4/6, IPv6, Ethernet), в поле **Первый адрес IPv4** ввести первый адрес из адресного пространства, в поле **Размер** указать размер адресного пространства и в поле **Первый MAC-адрес** ввести MAC-адрес для виртуальной сети (рисунок 140).

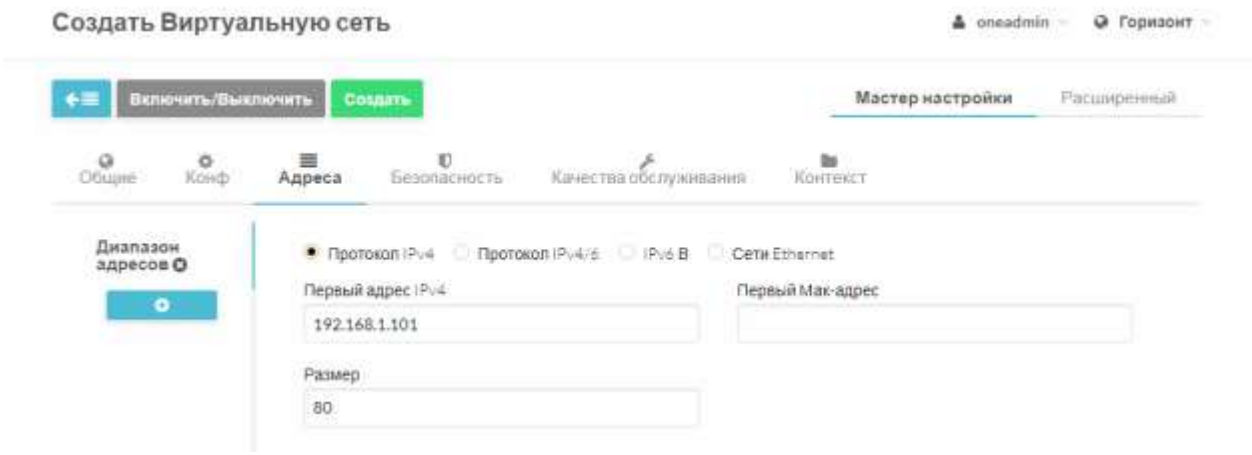


Рисунок 140 – Создание новой виртуальной сети. Вкладка «Адреса»

На вкладке **Безопасность** нужно из списка выбрать одну из групп безопасности (рисунок 141).

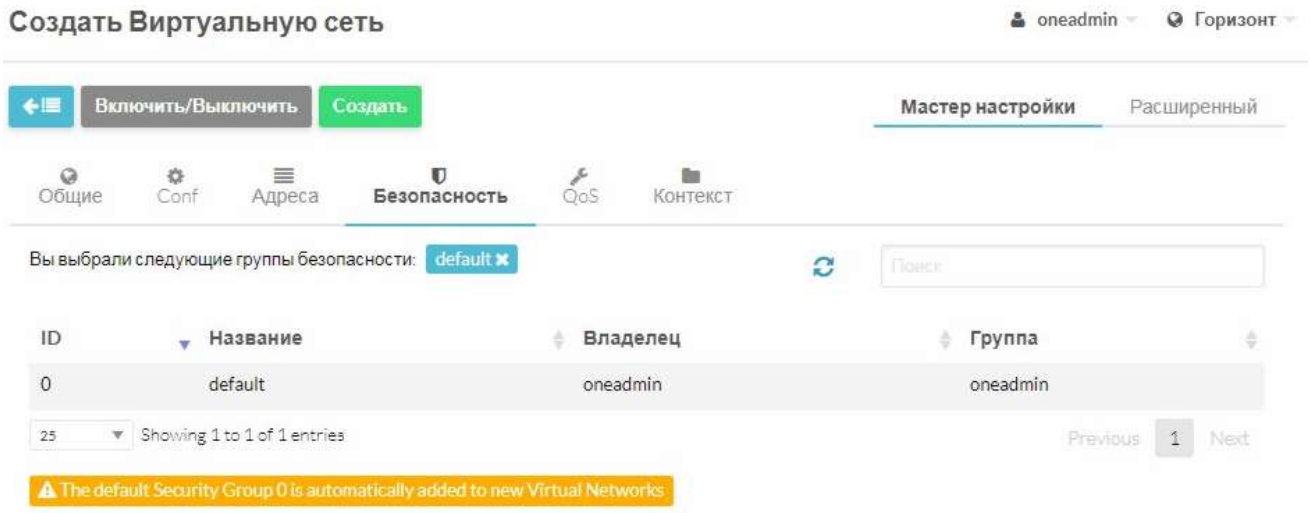


Рисунок 141 – Создание новой виртуальной сети. Вкладка «Безопасность»

На вкладке **Контекст** следует заполнить поля **Адрес сети**, **Маску подсети**, указать **Шлюз** (рисунок 142).

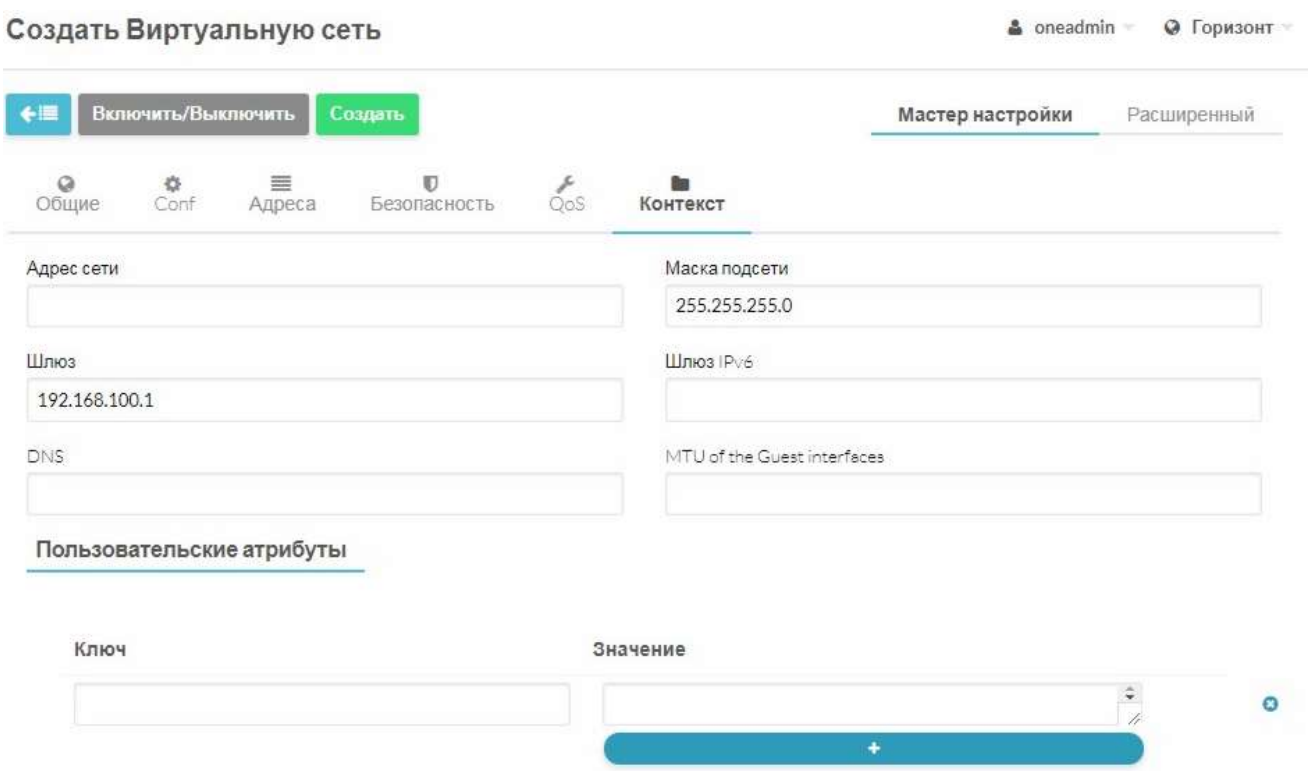


Рисунок 142 – Создание новой виртуальной сети. Вкладка «Контекст»

Если все данные введены верно, нужно нажать кнопку **Создать**. В окне **Виртуальные сети** (рисунок 143) появится новая сеть.

Для настройки виртуальных сетей необходимо в СГУ зайти в раздел *Сеть→Вирт. сети* и на экране отобразится список доступных виртуальных сетей и их свойства (рисунок 143).

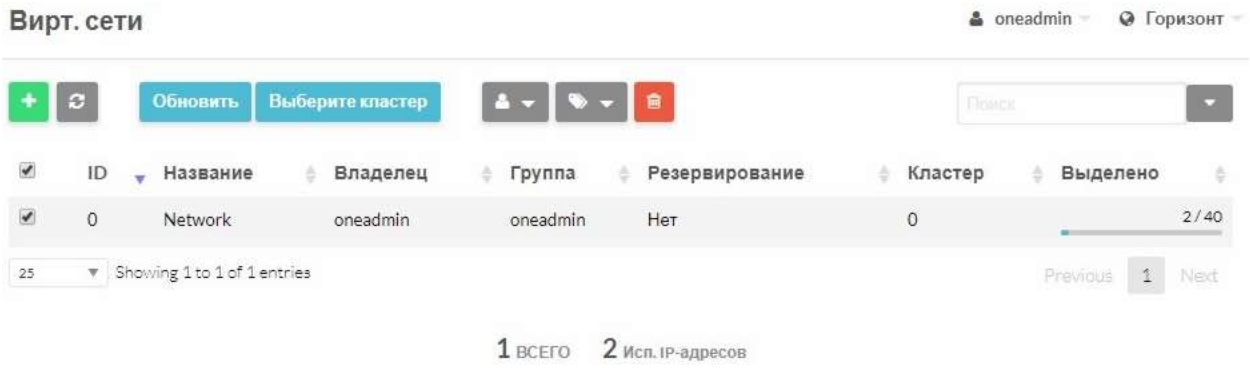


Рисунок 143 – Виртуальные сети

5.13 Создание шаблонов ВМ

Для конфигурации шаблона ВМ необходимо на панели управления шаблонами ВМ (раздел *Шаблоны ВМ→ВМ*) нажать кнопку . На экране откроется страница с мастером настройки конфигурации шаблона ВМ.

Мастер настройки представляет из себя систему вкладок, в которых предусмотрено моделирование конфигурации шаблона ВМ. По умолчанию открыта вкладка **Общие** (рисунок 144).

Вкладка **Общие** позволяет администратору дать наименование шаблону ВМ, составить дополнительное описание, а также для удобства пользования выбрать логотип гостевой ОС, планируемой для исполнения на ВМ.

В поле **Название** вводится наименование шаблона. В поле **Логотип** из выпадающего меню выбирается устанавливаемая гостевая ОС. В поле **Описание** вносится дополнительное описание шаблона ВМ (пример: «*ВМ отдела перспективных разработок. Базовое ПО, Win8, ОЗУ 8192 МБ, HardDisk 200 ГБ*»).

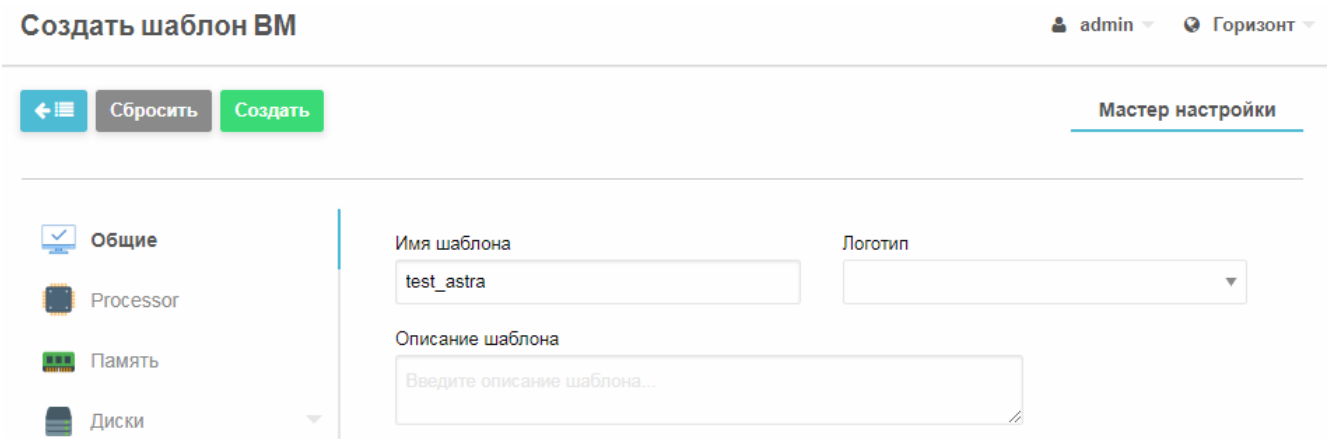


Рисунок 144 – Мастер настройки шаблона ВМ. Вкладка "Общие"

На вкладке **Процессор** настраивается конфигурация и архитектура ЦПУ (рисунок 145).

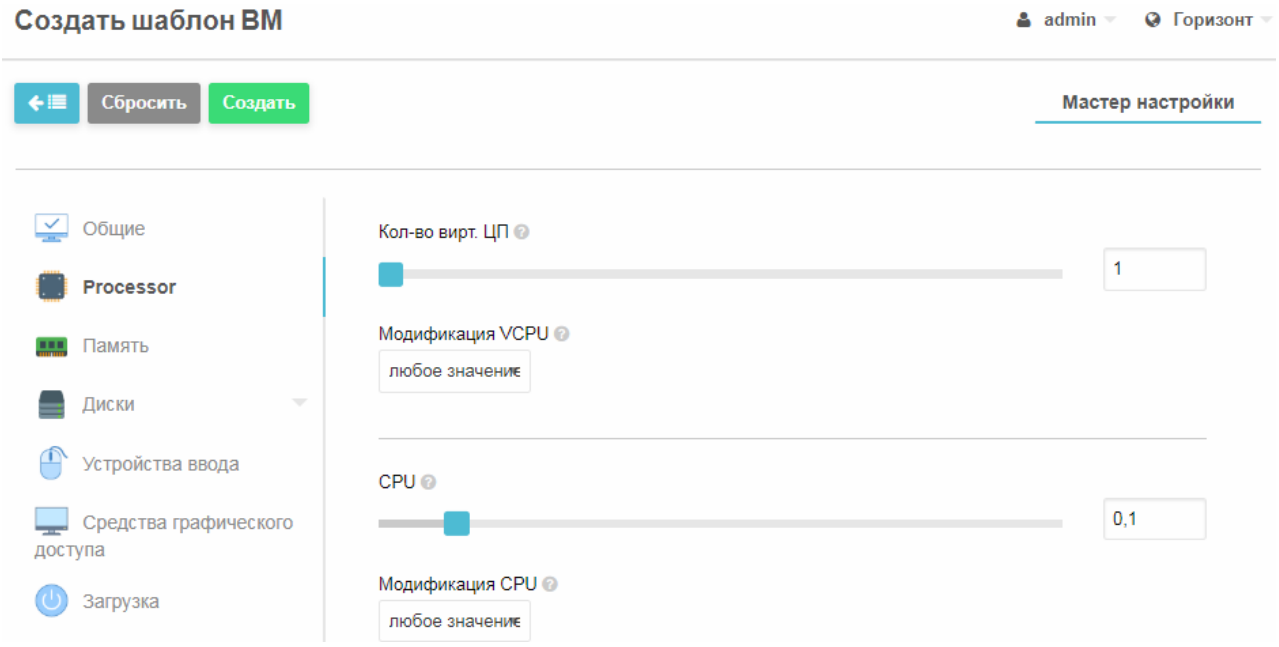


Рисунок 145 – Мастер настройки шаблона ВМ. Вкладка "Процессор"

В поле **Кол-во вирт. ЦП** с помощью ползунка или записью значения в окошко устанавливается количество виртуальных процессоров, необходимых для ВМ. По умолчанию устанавливается один виртуальный ЦП.

В поле **CPU** также с помощью ползунка или записью значения в окошко устанавливается доля процессорного времени, предоставляемая ВМ. Например, для выделения половины процессорного времени необходимо указать «*0,5*».

В поле **Модель процессора** выбрать модель процессора для создаваемого шаблона ВМ.

На вкладке **Память** устанавливается объем виртуальной оперативной памяти ВМ (рисунок 146).

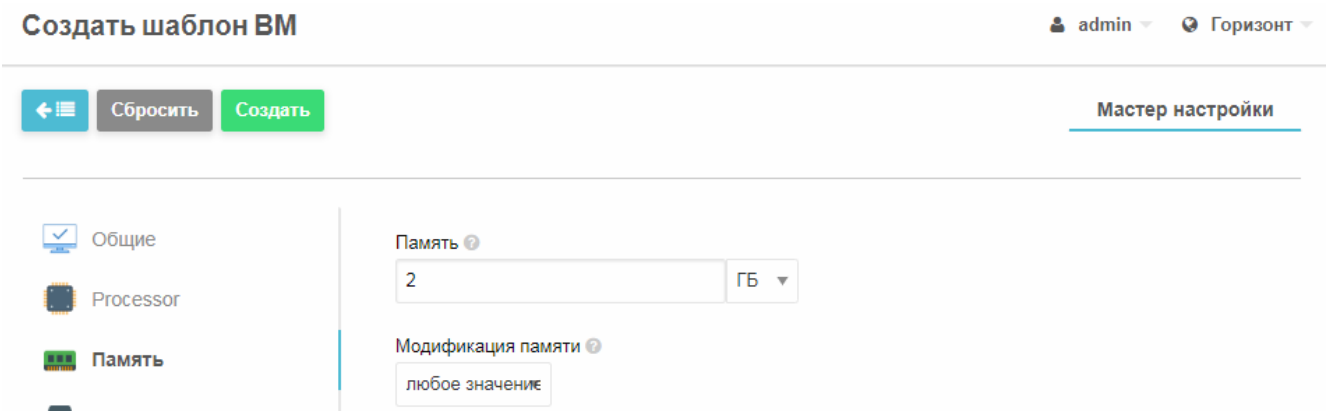


Рисунок 146 – Мастер настройки шаблона ВМ. Вкладка "Память"

В поле **Память** устанавливается объем ОЗУ, необходимый для ВМ. Параметр вносится либо целым числом в ГБ, либо кратным 512 в МБ.

На вкладке **Диски** (рисунок 147) к шаблону ВМ подсоединяются образы виртуальных жестких дисков или загрузочных дисков с гостевой ОС или другим ПО.

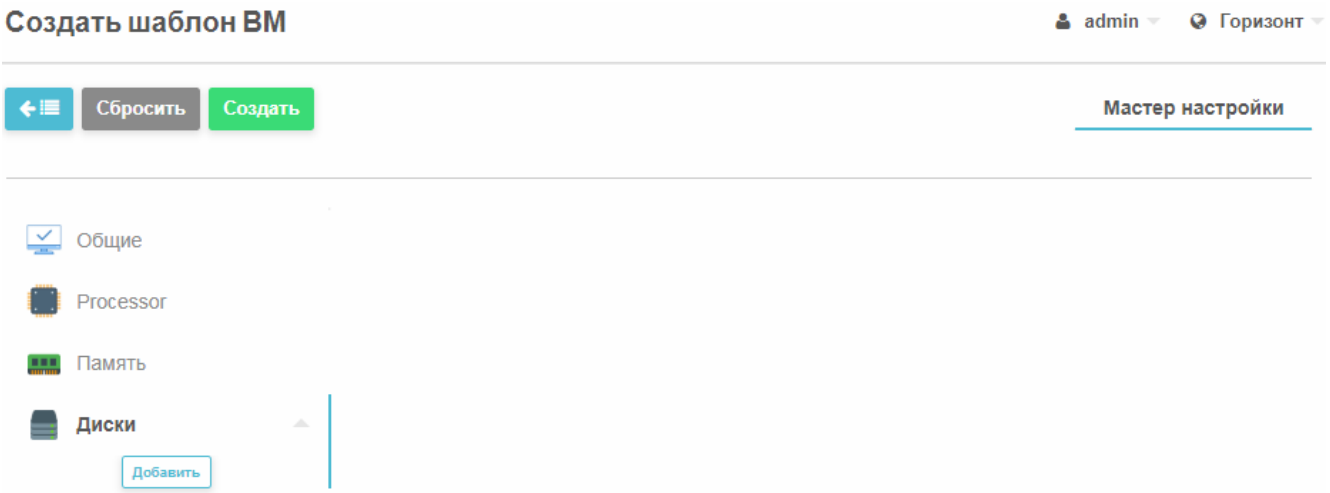


Рисунок 147 – Мастер настройки шаблона ВМ. Вкладка "Диски"

Для присоединения диска к ВМ необходимо нажать на кнопку **Добавить**. На вкладке **Диски** появится вкладка второго уровня VOLATILE, кликнув по которой откроется страница выбора и настройки подсоединяемого диска (рисунок 148).

Если необходимо подключить временный диск, то устанавливается соответствующий переключатель. В поле **Размер в ГБ** указывается необходимый размер жесткого диска в ГБ. В поле **Тип диска** выбирается тип файловой системы подсоединяемого диска: **FS** (Файловая система) или **SWAP**. В поле **Формат файловой системы** из раскрывающегося списка выбирается формат образа жесткого диска: **QCOW2** или **RAW** (рисунок 148).

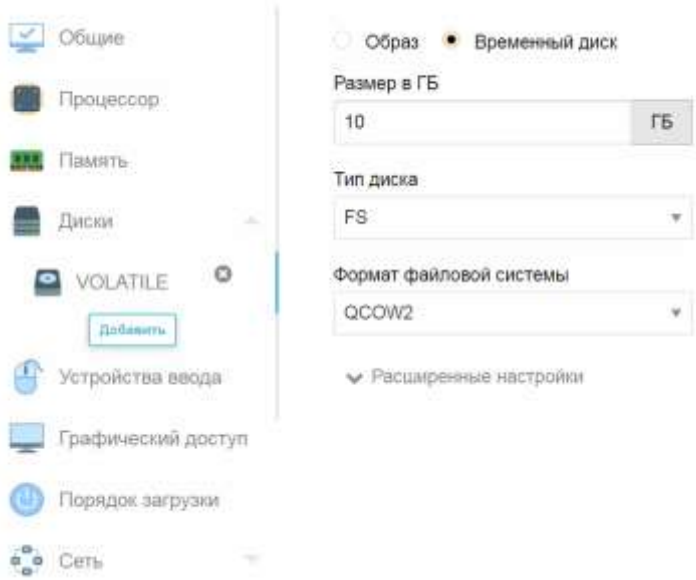


Рисунок 148 – Мастер настройки шаблона ВМ. Параметры дисков

Для выбора существующего образа диска активируется переключатель **Образ** и из списка образов выбирается искомый файл образа диска.

При выборе типа образа диска **Блок данных** вкладка второго уровня примет вид Блок данных. При выборе типа образа **CD-ROM** с установочным диском гостевой ОС или другим ПО вкладка второго уровня примет вид CDROM. При выборе типа образа диска **ОС** (образа жесткого диска с установленной гостевой ОС) вкладка второго уровня примет вид ОС. Выбранный образ отображается в строке **Вы выбрали следующий образ**.

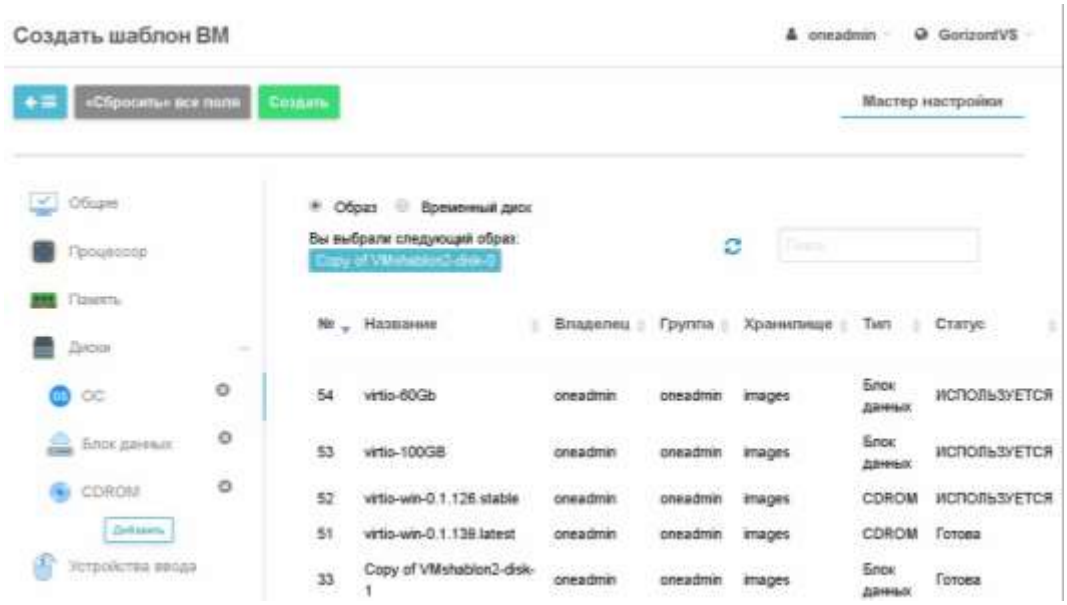


Рисунок 149 - Мастер настройки шаблона ВМ. Вкладка "Диски"

На вкладке **Устройства ввода** в поле **Тип** необходимо выбрать тип устройства ввода: **Мышь** или **Планшетный ПК**. В поле **Шина** из списка выбирается тип подсистемы архитектуры ВМ для передачи данных: **USB** или **PS/2**. После ввода всех данных следует нажать кнопку **Добавить** - на экране отобразится подсоединенное к ВМ устройство ввода.

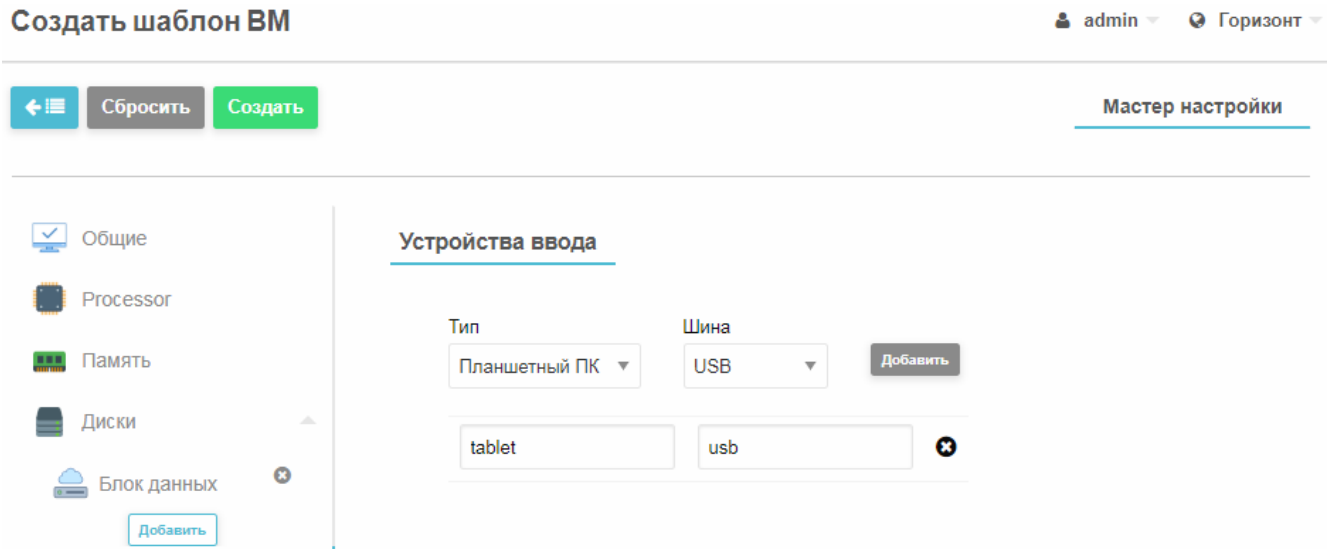


Рисунок 150 – Мастер настройки шаблона ВМ. Вкладка "Устройства ввода"

Рекомендуется для корректной работы манипулятора типа «мышь» на ВМ в поле **Тип** указать Планшетный ПК, в поле **Шина** – USB. После нажатия кнопки **Добавить** на экране появится подсоединенное к ВМ устройство ввода.

На вкладке **Sound** указывается тип аудиокарты, необходимый для ВМ.

На вкладке **Video** указывается тип видеокарты, необходимый для ВМ.

На вкладке **Графический доступ** указывается средства графического доступа, необходимые для ВМ: **VNC**, **SDL** или **SPICE** (рисунок 151).

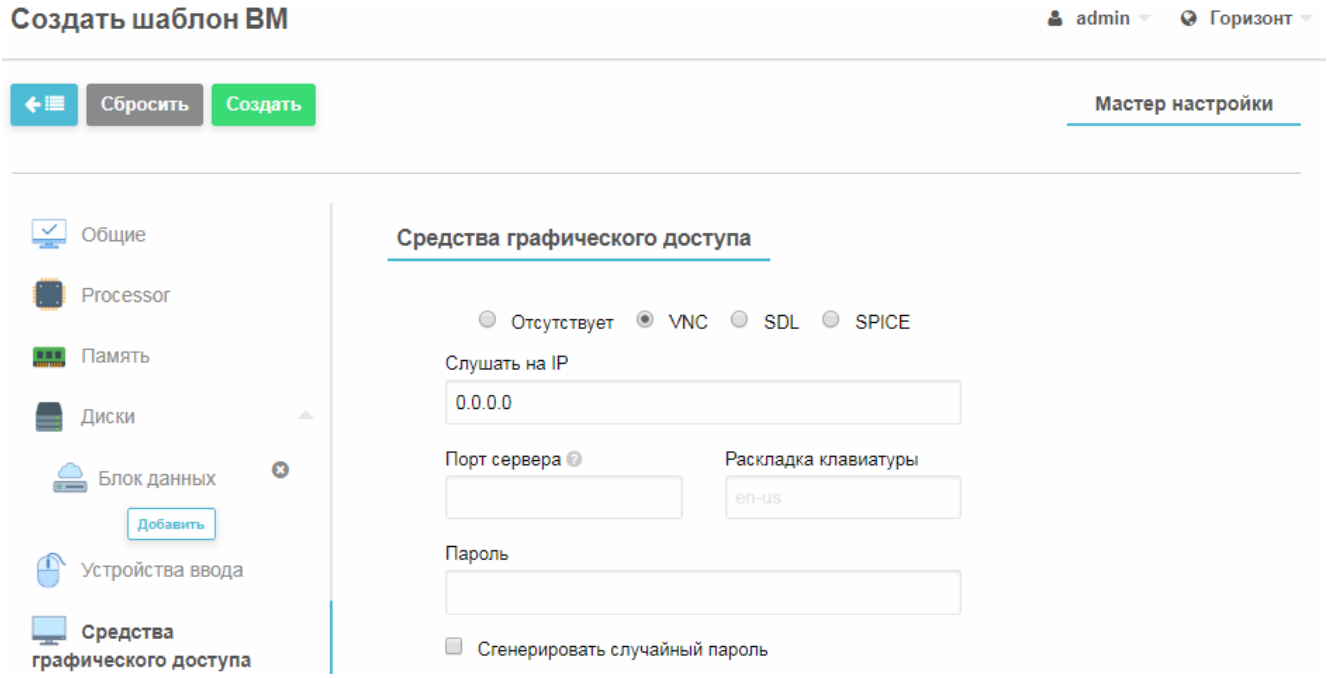


Рисунок 151 - Мастер настройки шаблона ВМ. Вкладка "Графический доступ"

На вкладке **Загрузка** (рисунок 152) необходимо выбрать загрузочные устройства и их порядок загрузки. Выбранные загрузочные устройства необходимо отметить флажком, а порядок их загрузки установить с помощью кнопок .

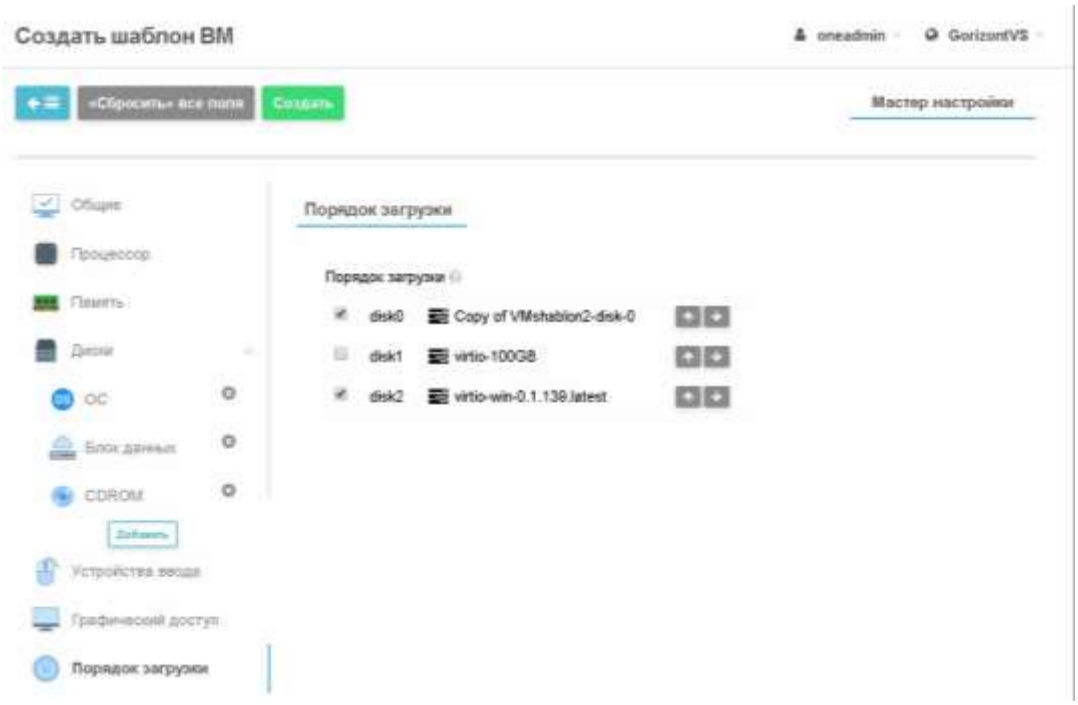


Рисунок 152 – Мастер настройки шаблона ВМ. Вкладка "Загрузка ОС"

Как показано на рисунке, сначала будет осуществлена загрузка с диска ***Copy of VMshablon2-disk-0*** с установленной гостевой операционной системой, затем будет

произведена загрузка ПО с ***virtio-win-0.1.139.latest*** – с образа оптического диска, установленного в виртуальный CD-ROM-привод.

На вкладке **Сеть** шаблон ВМ подключается к одной из виртуальных сетей. Для этого необходимо нажать кнопку **Добавить** и, кликнув по вкладке второго уровня NIC, выбрать интерфейс из созданных ранее виртуальных сетей (п. 5.12) (рисунок 153).

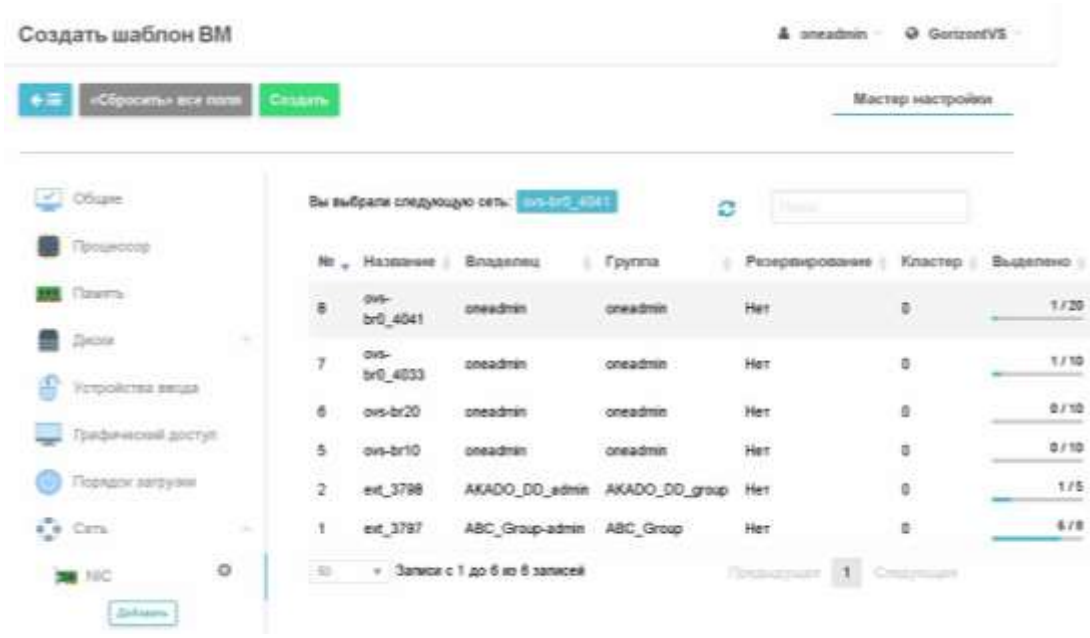


Рисунок 153 – Мастер настройки шаблона ВМ. Вкладка "Сеть"

При необходимости можно присоединить шаблон ВМ и к другим виртуальным сетям, созданным в системе. Для этого необходимо нажать кнопку **Добавить** и повторить процедуру выбора виртуальной сети.

5.14 Конфигурация шаблонов ВМ

5.14.1 Конфигурация шаблона ВМ на базе образа жесткого диска с данными

Для конфигурации шаблона ВМ на базе образа жесткого диска с данными (жесткого диска с установленной гостевой ОС) необходимо во вкладке **Диски** подсоединить к шаблону ВМ виртуальный жесткий диск с установленной гостевой ОС.

Для этого следует нажать кнопку **Добавить** и открыть вкладку второго уровня VOLATILE. В открывшемся окне отметить опцию **Образ** и выбирать созданный ранее qcow2-образ жесткого диска с установленной гостевой ОС (тип диска – **ОС**). При этом вкладка второго уровня примет вид ОС (рисунок 154).

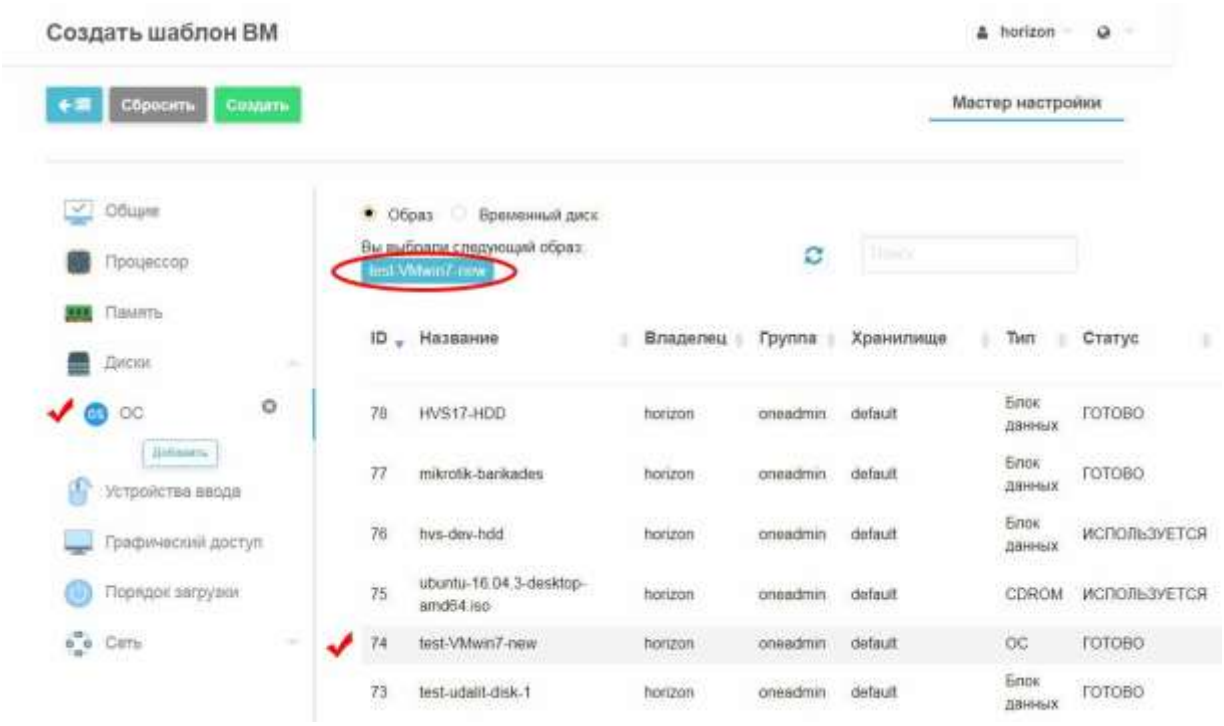


Рисунок 154 - Конфигурация шаблона ВМ

В случае необходимости присоединения к ВМ дополнительных вычислительных ресурсов, необходимо нажать кнопку **Добавить** и выбрать из образов дополнительный вычислительный ресурс. Например, второй жесткий диск под хранение данных. Для этого выбираем из предложенного перечня образов дисков пустого образ жесткого диска, созданного ранее (тип диска – **Блок данных**). При этом вкладка второго уровня примет вид 

(рисунок 155).

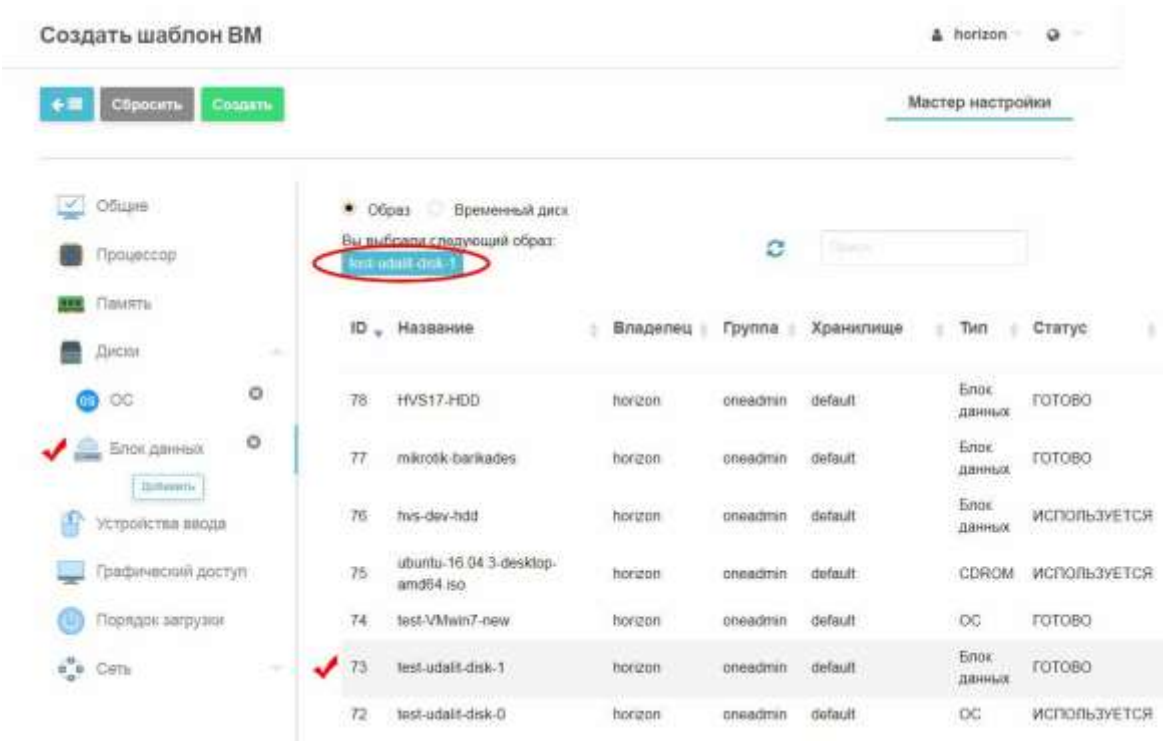


Рисунок 155 - Добавление ресурса к шаблону ВМ

После выбора образов устройств хранения информации, необходимых для ВМ, следует установить порядок загрузки ОС.

Для этого следует открыть вкладку **Порядок загрузки** и, установить флажок напротив образа диска с установленной ОС (рисунок 156).

Рисунок 156 - Установка порядка загрузки

Параметры в остальных вкладках указываются в соответствии с требованиями пользователя к создаваемому шаблону ВМ.

5.14.2 Конфигурация шаблона ВМ на базе образа CD-ROM с ОС

Для конфигурации шаблона ВМ на базе образа CD-ROM с ОС необходимо во вкладке **Диски** подсоединить к шаблону ВМ виртуальный дисководов CD-ROM с диском для инсталляции на ВМ дистрибутива операционной системы.

Для этого следует нажать кнопку **Добавить** и открыть вкладку второго уровня VOLATILE. В открывшемся окне отметить опцию **Образ** и выбрать созданный ранее iso-образ CD-ROM с ОС (тип диска – ***CDROM***). При этом вкладка второго уровня примет вид CDROM.

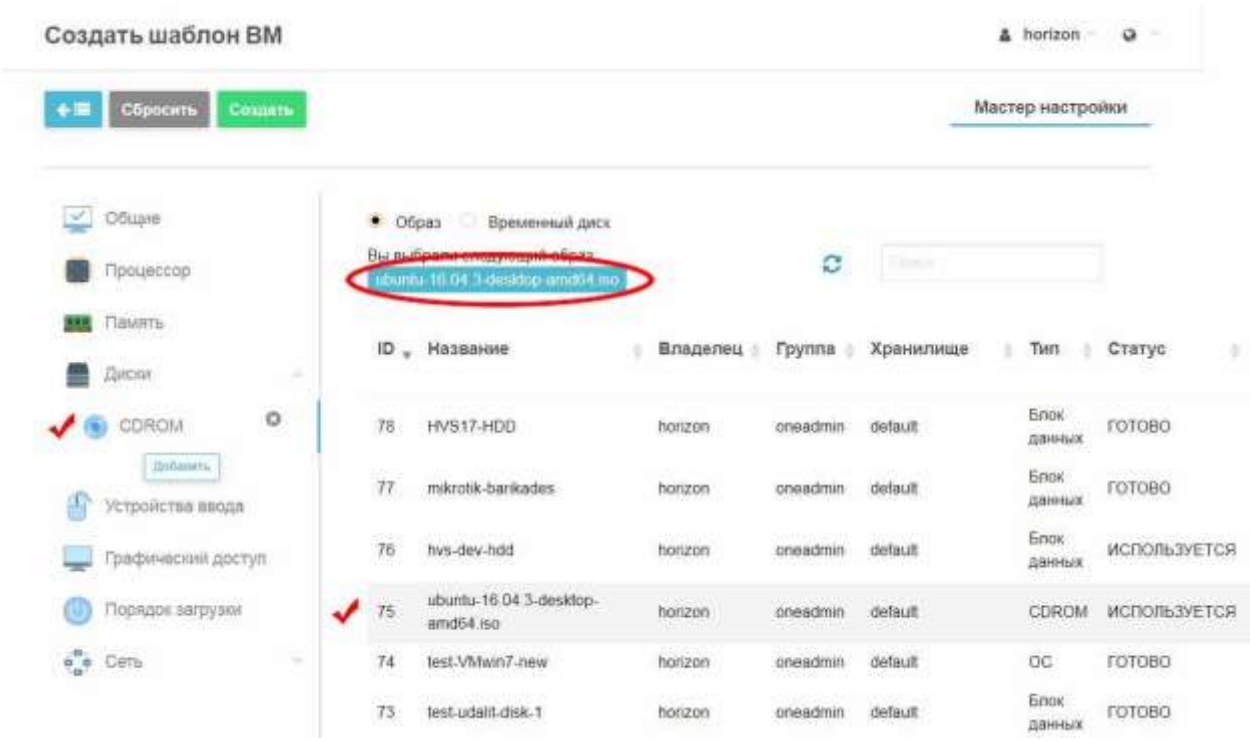


Рисунок 157 - Конфигурация шаблона ВМ на базе образа CD-ROM с ОС

Далее необходимо присоединить к ВМ образ жесткого диска на который будет устанавливаться ОС. Для этого нажать кнопку **Добавить** и выбрать из предложенного перечня образов дисков пустой образ жесткого диска, созданного ранее (тип диска – ***Блок данных***), на который будет устанавливаться операционная система. При этом вкладка второго уровня примет вид 

.

В случае возникновения потребности подсоединить к ВМ дополнительные вычислительные ресурсы, необходимо повторить процедуру добавления пустого образа жесткого диска, описанную выше.

После выбора образов устройств хранения информации, необходимых для ВМ, следует установить порядок загрузки ОС. Для этого открыть вкладку **Порядок загрузки** и, установить флажок напротив iso-образа CD-ROM с ОС.

5.15 Изменение конфигурации шаблонов ВМ

Для изменения конфигурации шаблона ВМ необходимо в разделе *Шаблоны* подразделе *ВМ* в таблице кликнуть по изменяемому шаблону левой клавишей “мыши” - откроется информационное окно с параметрами шаблона ВМ (рисунок 158).

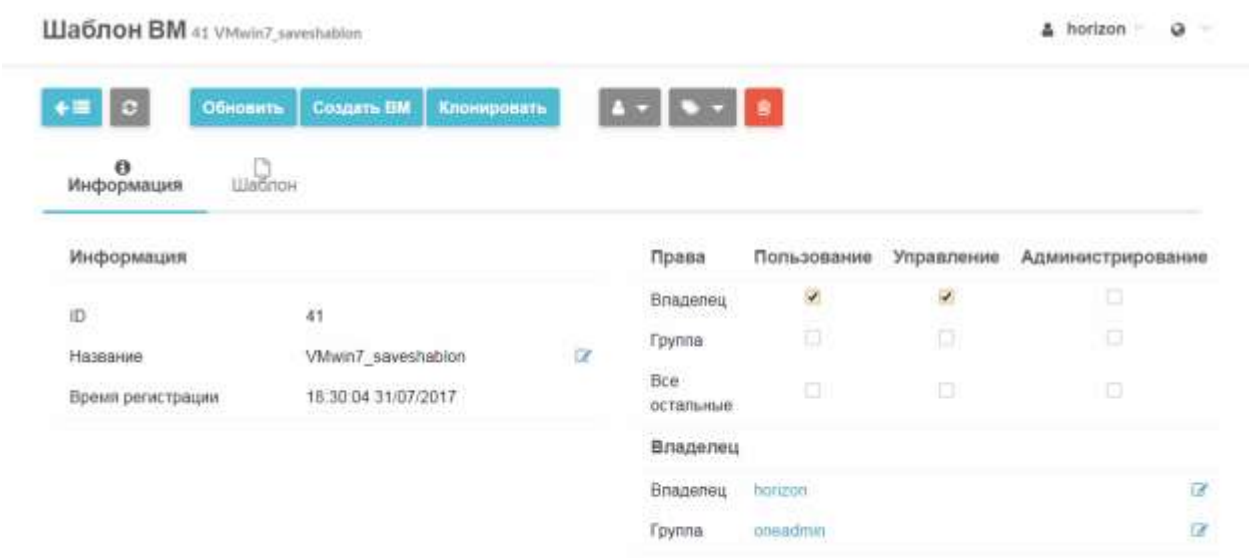


Рисунок 158 - Окно параметров шаблона ВМ

На вкладке **Информация** есть возможность изменить название шаблона, права доступа, владельца шаблона, а также группу пользователей шаблоном.

Кроме того, станет активной панель управления конфигурацией шаблона ВМ.

С помощью панели управления шаблоном ВМ пользователь может создать ВМ на базе этого шаблона ВМ, клонировать шаблон (сделать копию шаблона), а также изменить конфигурацию шаблона.

После нажатия кнопки **Обновить** пользователь попадает в мастера изменения настройки шаблона ВМ, аналогичному мастеру создания шаблона ВМ, описанному в п. 5.13.

5.16 Создание ВМ на основе шаблона

Для создания ВМ необходимо в разделе *Машины* выбрать подраздел *ВМ* и нажать кнопку .

В открывшемся окне выбрать необходимый шаблон ВМ (создание шаблона описано в п. 5.13), после чего на странице откроются дополнительные опции: имя ВМ, количество экземпляров, создаваемых ВМ, производительность и подсоединенные виртуальные диски. После заполнения всех полей необходимо нажать кнопку **Создать** (рисунок 159).

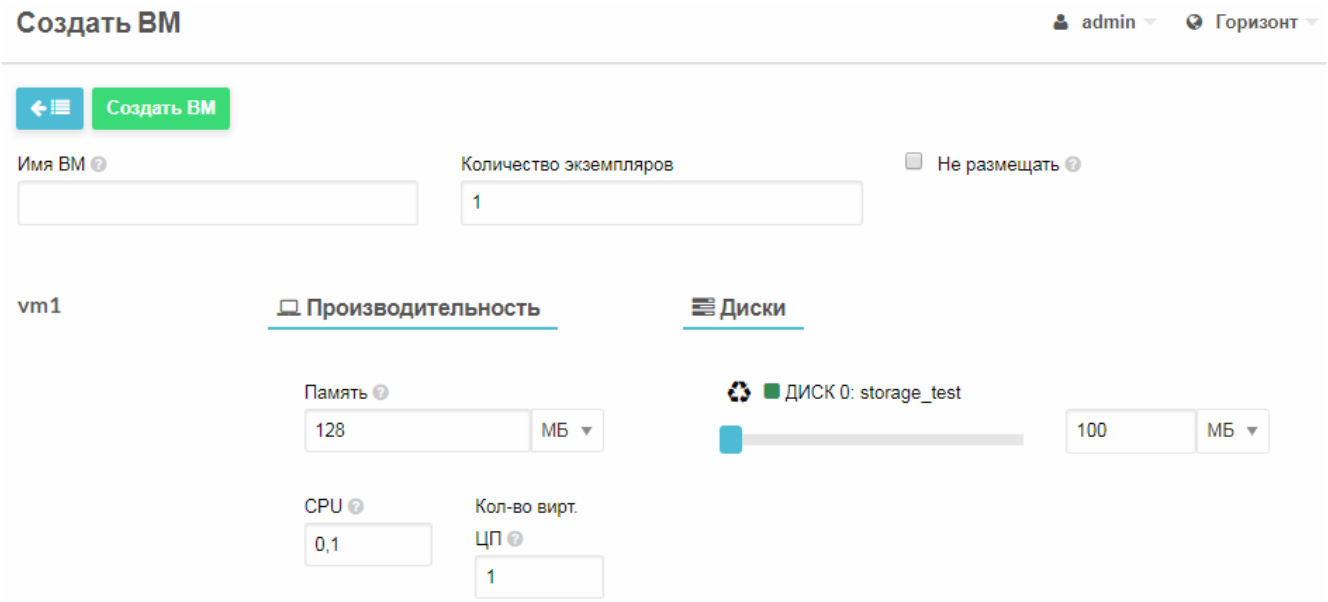


Рисунок 159 – Создание ВМ

Размещение ВМ на узле происходит автоматически, после чего у ВМ появится статус *Выполняется*.

Дополнительно в разделе *Машины*, подразделе *ВМ*, панели управления можно указать метку для созданной ВМ (например, «*ВМ отдела маркетинга*») (рисунок 160).

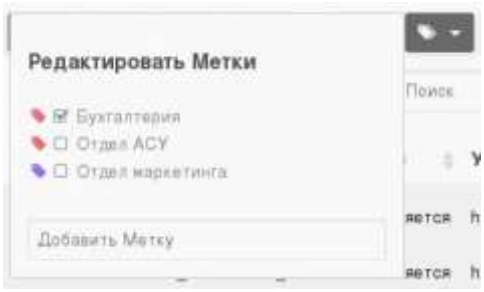


Рисунок 160 – Метки ВМ

Если в шаблоне был указан порядок загрузки ОС с виртуального дисковода CD-ROM, то в ВМ начнется процесс установки гостевой ОС.

После установки гостевой ОС можно создать шаблон ВМ с уже установленной ОС. Для этого необходимо выключить ВМ и в панели управления виртуальной машиной нажать кнопку  .

Для работы с ВМ в отдельной вкладке браузера следует нажать на иконку  , откроется окно рабочего стола ВМ (рисунок 161).

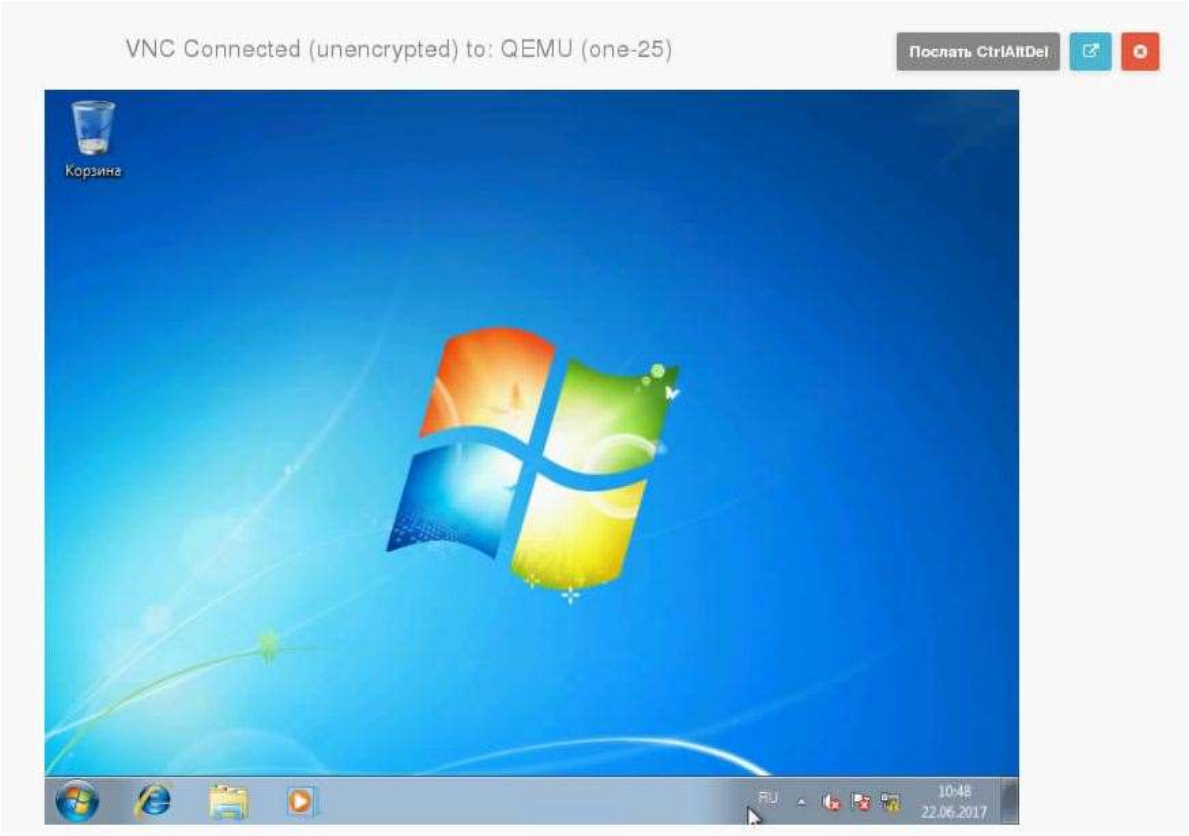


Рисунок 161 – Вид рабочего стола гостевой ОС

5.17 Управление ВМ при помощи СГУ

При выборе одной и более ВМ (рисунок 162) в разделе *Экземпляры ВМ→ВМ* становится активной панель управления ВМ. Осуществлять управление возможно, как отдельной ВМ, так и предварительной выделенной группой ВМ.

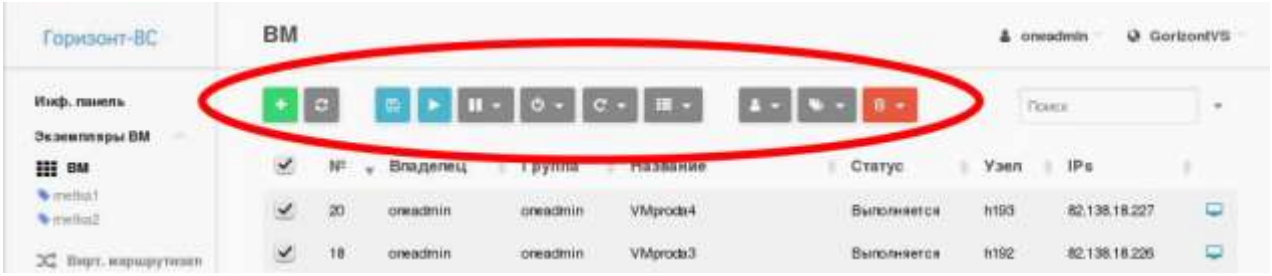


Рисунок 162 - Панель управления ВМ

Подробно функционал описан в таблице 1.

Таблица 1 - Команды панели управления ВМ

Опция	Функция	Описание
	Создание новой ВМ (активна всегда)	Открывается страницу интерфейса создания новой ВМ.
	Обновление текущей страницы (активна всегда)	После внесения каких-либо изменений в работу ВМ или ее конфигурацию необходимо выполнить обновление страницы, чтобы увидеть изменения.

Опция	Функция	Описание
	Создание шаблона ВМ на базе существующей ВМ	Позволяет создать шаблон с параметрами и конфигурацией существующей ВМ. *Примечание. ВМ во время создания шаблона должна быть выключена.*
	Запуск ВМ	На ВМ инициализируется запуск гостевой ОС.
	**Выпадающее меню:**	
	Приостановить работу ВМ	Работа ВМ приостанавливается. ВМ может быть запущенна в любой момент времени с текущего состояния до приостановки работы ВМ.
	Остановить	Работа ВМ останавливается. Оперативная память записывается на жесткий диск. Работа ВМ может быть запущена в любой момент времени с текущего состояния до остановки ВМ.
	**Выпадающее меню:**	
	- Отключить питание	Корректное выключение ВМ из системы группового управления
	- Отключить питание hard	Принудительное отключение питания ВМ. Отключение питания ВМ из системы группового управления (аналогично некорректному выключению физической машины посредством отключения питания из сети).
	- Отменить размещение	ВМ снимается с узла и сохраняется в хранилище в виде файла-образа ВМ с возможностью восстановления. Восстановление ВМ осуществляется непосредственно размещением ее на серверном узле или нажатием кнопки запуска ВМ (в этом случае происходит автоматическое размещение ВМ на узле)
	- Отменить размещение hard	ВМ снимается с узла и сохраняется на физическом сервере в виде файла-образа ВМ с возможностью восстановления. Восстановление ВМ происходит так, как будто она создается заново. Происходит ее размещение на узле.
	**Выпадающее меню:**	
	- Перезагрузка	Корректная перезагрузка гостевой ОС на ВМ (аналогична перезагрузки из меню «Пуск»)
	- Перезагрузка hard	Принудительная перезагрузка гостевой ОС на ВМ (аналогична перезагрузке через кнопку «reset»)
	**Выпадающее меню:**	
	- Разместить на узле	Ручное размещение ВМ на узле с возможностью выбора узла размещения.
	- Перенести ВМ	Миграция ВМ между узлами
	- Перенести ВМ live	Горячая миграция ВМ между узлами
	- Восстановить	Восстановление ВМ. Позволяет - retry – - успешно –

Опция	Функция	Описание
		- не выполнено – - удалить – удаляет ВМ из системы; - удалить и создать повторно – удаляет ВМ из системы, а затем корректно развертывает в системе аналогичную ВМ.
	**Выпадающее меню:**	
	- Сменить владельца	Позволяет сменить пользователя ВМ
	- Сменить группу	Позволяет сменить группу пользователей
	Добавить метку	Для удобства управления ВМ в системе группового управления предусмотрены метки, которые позволяют группировать и выводить списки виртуальных машин по их типу или функциональному предназначению. Например: ВМ бухгалтерии, ВМ отдела АСУ и т.д.
	**Выпадающее меню:**	
	- Уничтожить	Корректное удаление ВМ из системы
	- Уничтожить hard	Принудительное удаление ВМ из системы

5.18 Редактирование параметров ВМ

Для изменения параметров ВМ необходимо перейти в раздел *Экземпляры ВМ→ВМ*, кликнуть левой кнопкой “мыши” по выбранной ВМ. Откроется окно со вкладками параметров, информацией и данными виртуальной машины (рисунок 163), при этом останется доступной и панель управления, описанная в п. 5.17.

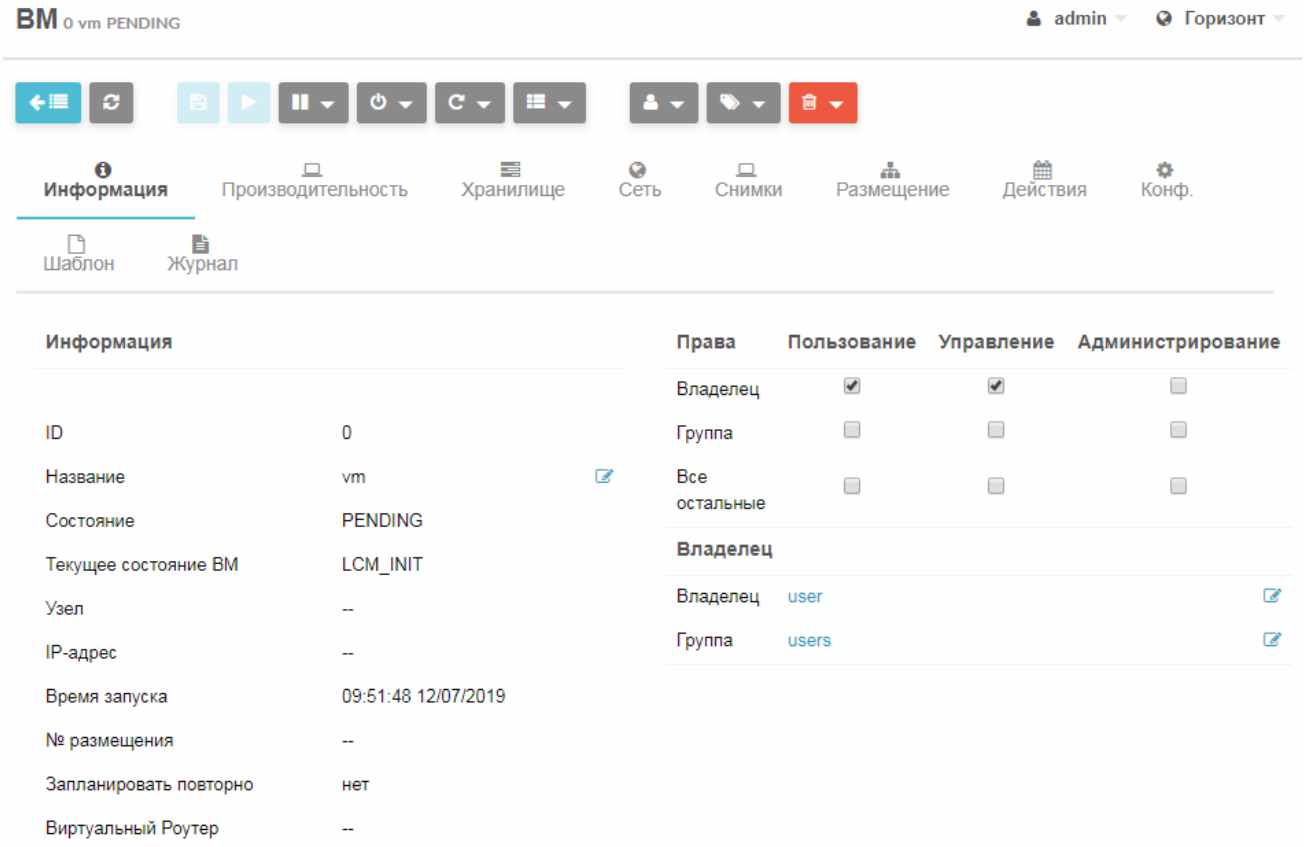


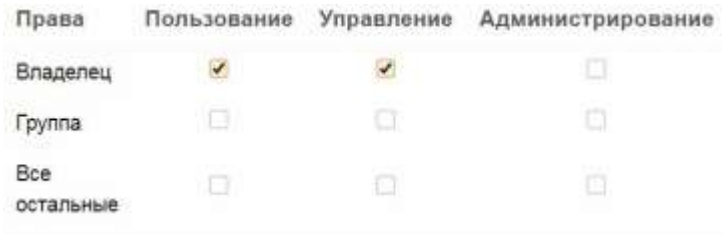
Рисунок 163 – Редактирование параметров ВМ

5.18.1 Вкладка “Информация”

На вкладке **Информация** в разделе **Информация** есть возможность изменить название ВМ. Для этого необходимо напротив параметра **Название** кликнуть по значку  и в появившемся поле  ввести новое название ВМ.

Кроме того, на вкладке представлена общая информация о ВМ: номер, название, состояние ЦПУ, текущее состояние ВМ, IP-адрес узла размещения, IP-адрес ВМ, время запуска.

На вкладке **Информация** представлена матрица дискреционного разграничения прав доступа к ВМ: пользования, управления, администрирования. Соответствующее право доступа может быть предоставлено владельцу ВМ (**Владелец**), группе пользователей (**Группа**) и всем пользователям, зарегистрированным в СГУ (**Все остальные**).



Права	Пользование	Управление	Администрирование
Владелец	☑	☑	☐
Группа	☐	☐	☐
Все остальные	☐	☐	☐

Для изменения прав доступа необходимо поставить/снять флажок в нужном поле.

В разделе **Владелец** представлен владелец ВМ и группа пользователей, которым могут быть делегированы те или иные права доступа к ВМ (по умолчанию в поле **Группа** стоит название группы, к которой принадлежит пользователь).

Для изменения владельца ВМ или группы пользователей ВМ, необходимо кликнуть по значку  и выбрать из выпадающего списка новый параметр.

5.18.2 Вкладка “Производительность”

На вкладке **Производительность** предоставляется возможность изменить базовые характеристики ВМ (рисунок 164).

Рисунок 164 - Вкладка "Производительность"

Примечание: *Виртуальная машина во время изменения базовых характеристик должна быть выключена.*

Для этого необходимо нажать на кнопку **Применить** и в окне **Изменить базовые характеристики** внести новые параметры ВМ: объем оперативной памяти, процент процессорного времени ЦП и количество виртуальных ЦП, и снова нажать кнопку **Применить** (рисунок 165).

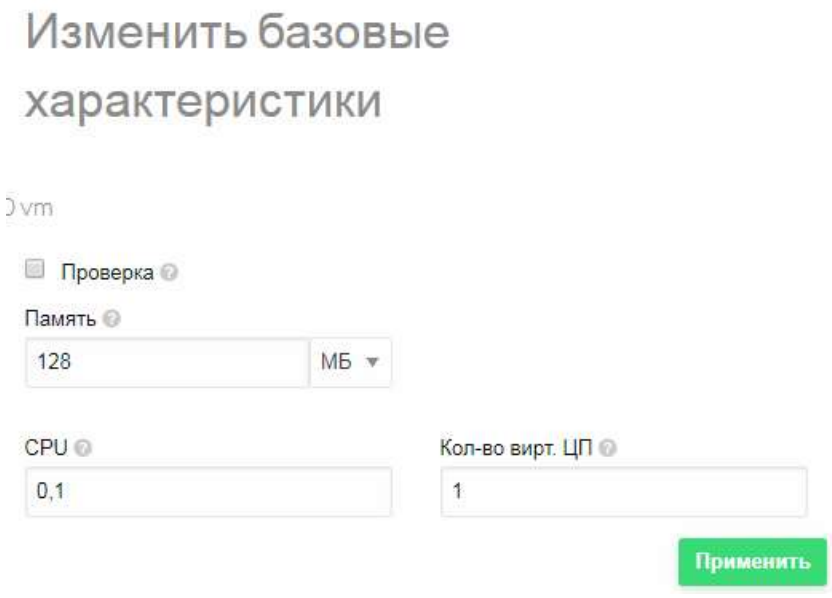


Рисунок 165 - Изменение базовых характеристик

Кроме того, в нижней части вкладки **Производительность** в виде графика представлен мониторинг реального использования процента процессорного времени и оперативной памяти по сравнению с выделенными параметрами для работы ВМ.

5.18.3 Вкладка “Хранилище”

На вкладке **Хранилище** есть возможно присоединить к ВМ новые ресурсы (пустые образы жестких дисков, CDROM-образы, образы ОС, временные диски), а также провести ряд манипуляций с присоединенными ресурсами к ВМ по отдельности (рисунок 166).

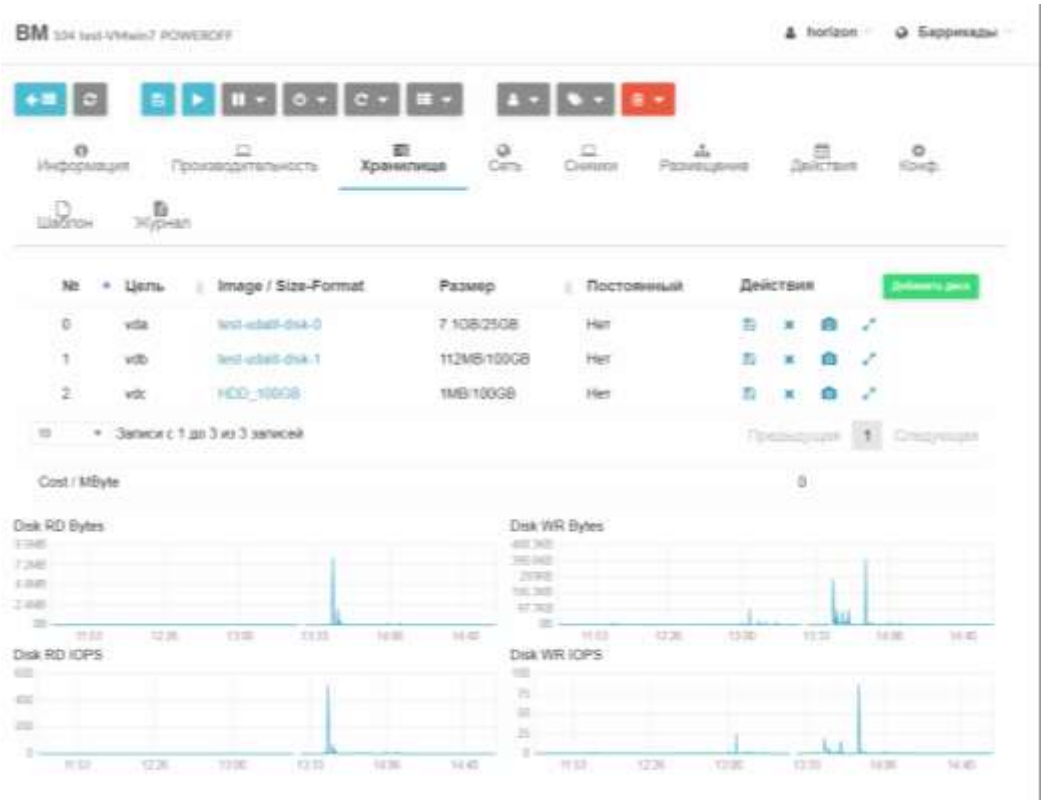


Рисунок 166 - Вкладка "Хранилище"

Для присоединения дополнительного ресурса необходимо нажать кнопку **Добавить диск**. В открывшемся окне **Присоединить диск** (рисунок 167) из предложенного списка выбрать образ требуемого ресурса и нажать кнопку **Присоединить**.

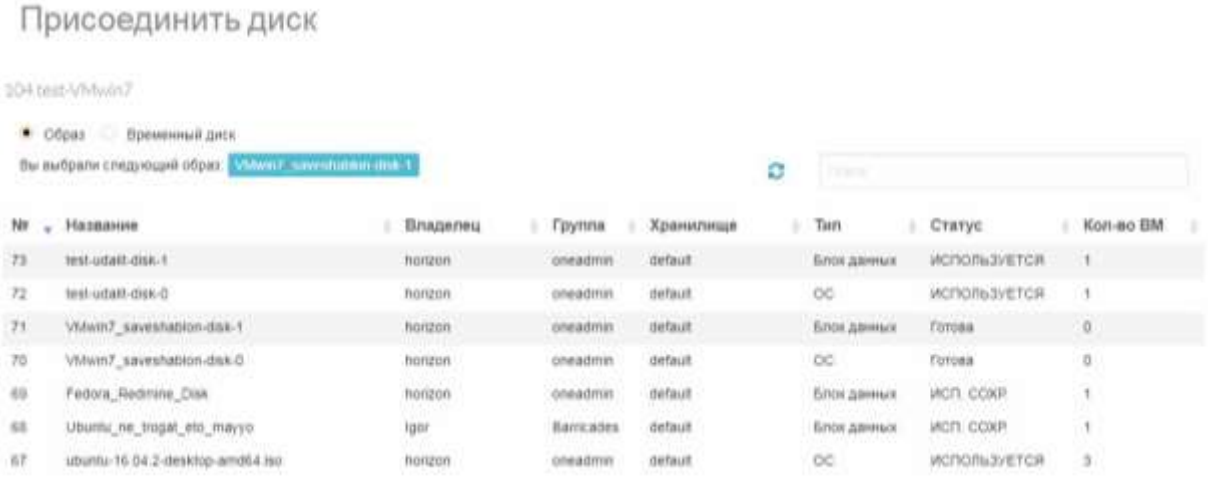


Рисунок 167 - Присоединить диск к ВМ

Для совершения дополнительных действий над присоединенными ресурсами к ВМ необходимо в столбце **Действия** (рисунок 166) выбрать одну из опций:

- создание образа диска из одного из ресурсов ВМ (подробнее см. п. 5.18.4);
- удаления ресурса;
- создание снимка из одного из ресурсов ВМ (подробнее см. п. 5.18.5);
- изменение объема дискового пространства (подробнее см. п. 5.18.6).

***Примечание**: опция активна только при выключенной ВМ*.

Кроме того, в нижней части вкладки **Хранилище** информационно в виде графика представлен мониторинг взаимодействия ВМ с дисковой подсистемой: скорость чтения (RD Bytes) и записи (WR Bytes) на жесткий диск байт в секунду и количество операций ввода/вывода в секунду (IOPS) при чтении (RD IOPS) и записи (WR IOPS) информации на жесткий диск.

5.18.4 Создание образа диска из одного из ресурсов ВМ

Для создания образа диска из одного из исполняемых жестких дисков ВМ необходимо активировать опцию в строке исходного жесткого диска (рисунок 166).

На экране откроется окно создания образа, в котором необходимо ввести имя нового образа диска и нажать кнопку **Сохранить как** (рисунок 168).

Рисунок 168 - Сохранение жесткого диска

После чего в разделе СГУ *Хранилище→Образы ВМ* разместится новый образ жесткого диска, на базе которого возможно создание нового шаблона ВМ (рисунок 169).

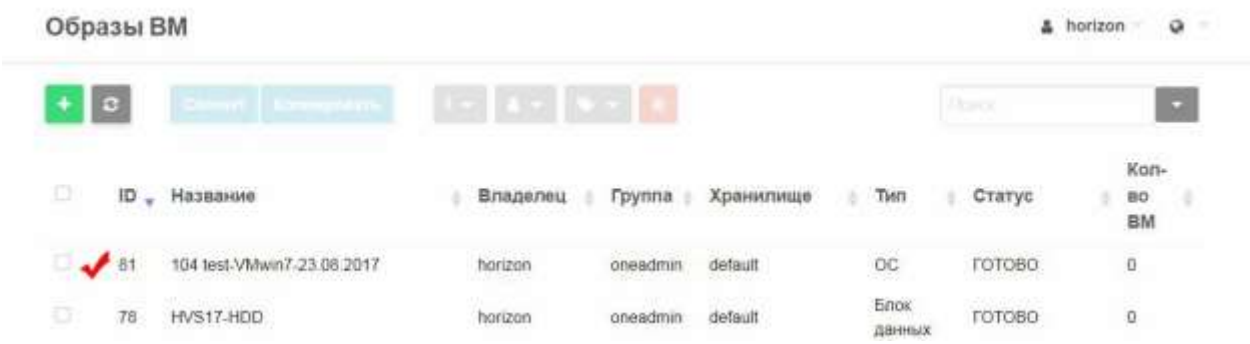


Рисунок 169

5.18.5 Создание снимка из одного из ресурсов ВМ

Для создания снимка одного из ресурсов ВМ необходимо сначала остановить ВМ, а затем активировать опцию в строке исходного жесткого диска.

На экране откроется окно **Снимок диска** (рисунок 170), в котором необходимо ввести имя снимка и нажать кнопку **Сделать снимок**.

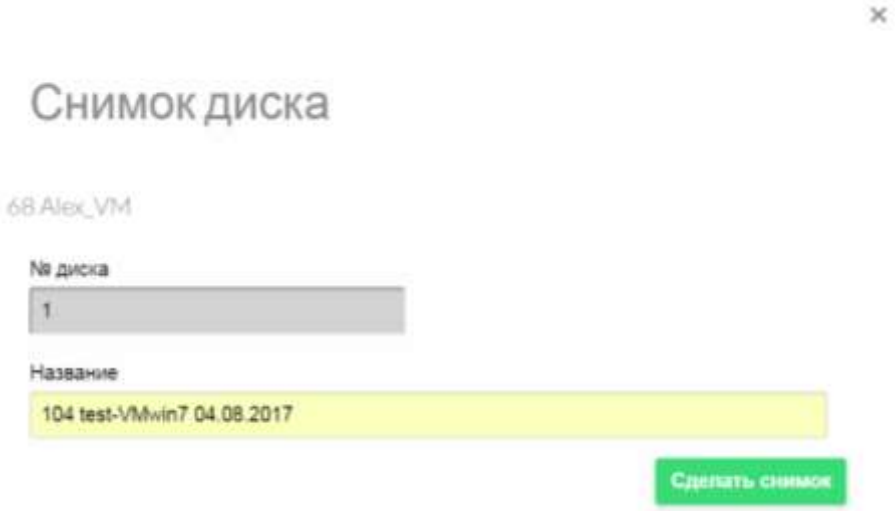


Рисунок 170 - Снимок диска

После чего в таблице на вкладке **Хранилище** диск, с которого был сделан снимок, будет отмечен знаком , после нажатия на который появится информация о сделанном снимке (рисунок 171).

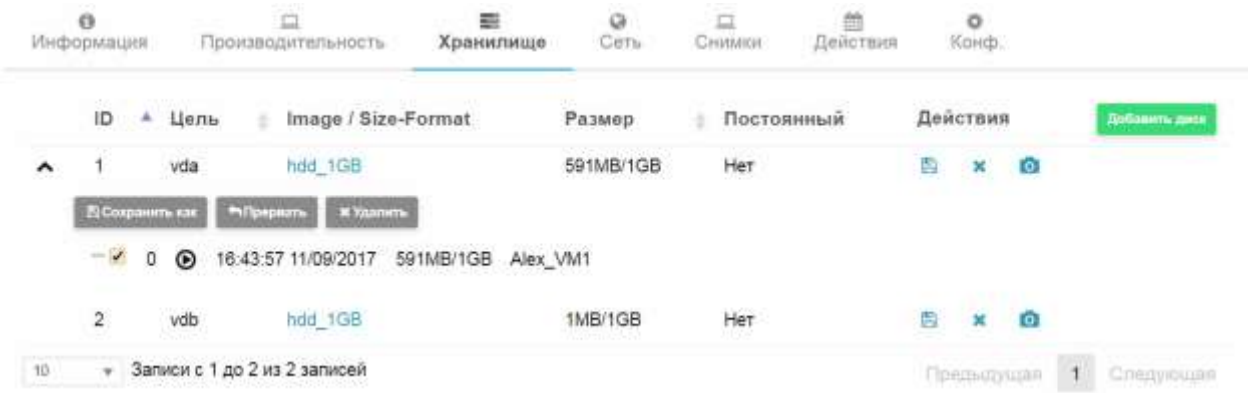


Рисунок 171 - Работа со снимком диска

Для сделанного снимка доступны следующие операции:

- сделать образ диска, нажав кнопку **Сохранить как**;
- возвратить диск на момент совершения снимка, нажав кнопку **Прервать**;
- удалить снимок, нажав кнопку **Удалить**.

5.18.6 Изменение объема дискового пространства

Для изменения объема дискового пространства (*опция активна только при выключенной ВМ*) необходимо активизировать опцию в строке изменяемого жесткого диска.

На экране откроется окно изменения дискового пространства (рисунок 172), в котором необходимо с помощью ползунка установить требуемое дисковое пространство для диска и нажать кнопку **Применить**.

Рисунок 172 – Окно изменения дискового пространства

После чего пользователь во вкладке **Хранилище** может удостовериться, что у выбранного диска изменился объем дискового пространства согласно введенному параметру.

5.18.7 Вкладка “Сеть”

На вкладке **Сеть** есть возможность добавить или отсоединить сетевой интерфейс (рисунок 173).

Рисунок 173 – Вкладка "Сеть"

Для добавления нового сетевого интерфейса необходимо нажать кнопку **Добавить сетевой интерфейс**. В открывшемся окне **Добавить сетевой интерфейс** (рисунок 174) выбрать из списка не менее одного сетевого интерфейса и нажать кнопку **Присоединить**.

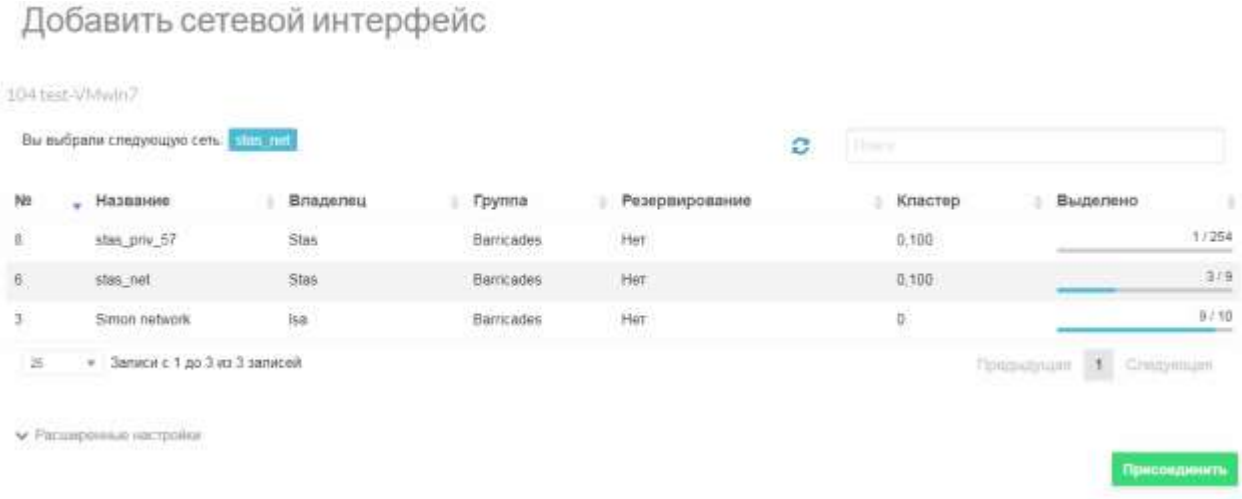


Рисунок 174 - Добавить сетевой интерфейс в ВМ

Для отсоединения сетевого интерфейса необходимо в столбце со списком присоединенных интерфейсов (рисунок 173) выбрать опцию **Отсоединить**.

В нижней части вкладки **Сеть** в виде графика представлен мониторинг работы сети: прием и передача данных (KB, MB), скорость входящих и исходящих соединений (B/s).

5.18.8 Вкладка “Действия”

На вкладке **Действия** есть возможность запланировать ряд отложенных манипуляций над ВМ, которые будут выполнены в автоматическом режиме.

Для того, чтобы запланировать действие (или ряд действий), необходимо нажать кнопку **Добавить действие**. На экране появится выпадающее меню с выбором действий (рисунок 175).

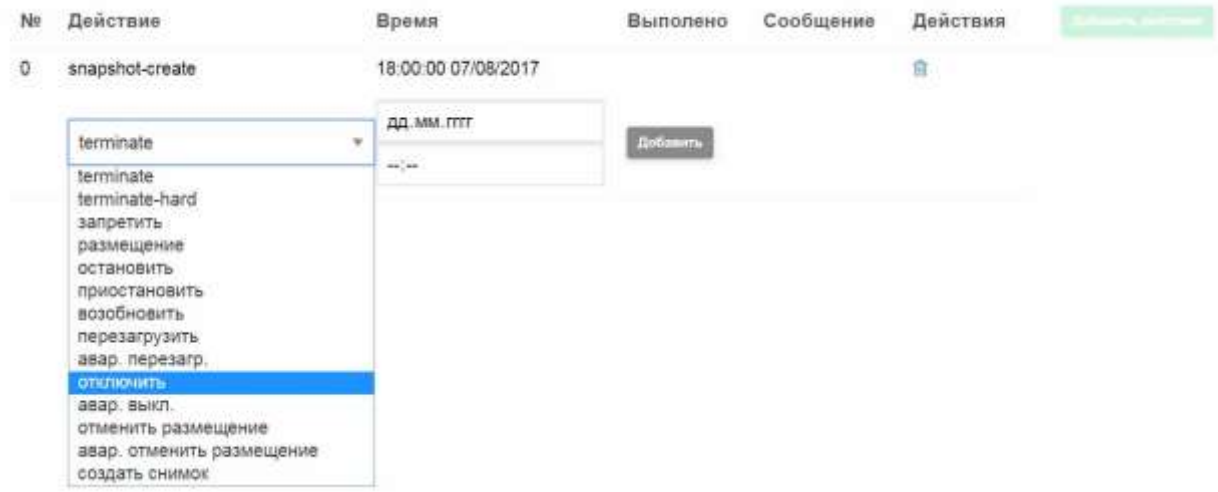
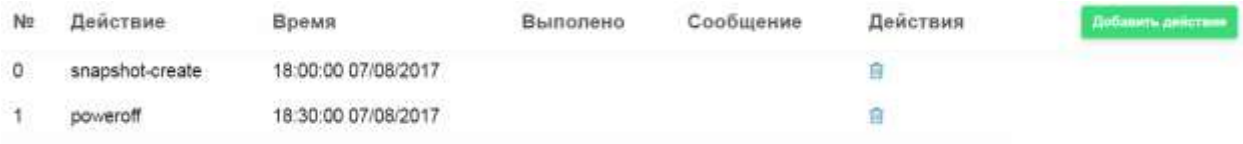


Рисунок 175 - Добавление действий

Необходимо выбрать требуемое действие, установить дату и время его выполнения и нажать кнопку **Добавить**. На странице появиться запись о запланированном действии и время его исполнения.



Для планирования нескольких действий необходимо повторить процедуру добавления действия.

5.18.9 Вкладка “Конфигурация”

На вкладке **Конф.** Есть возможность изменить конфигурацию ВМ (рисунок 176).

Примечание: *при изменении конфигурации ВМ должна быть выключена*.

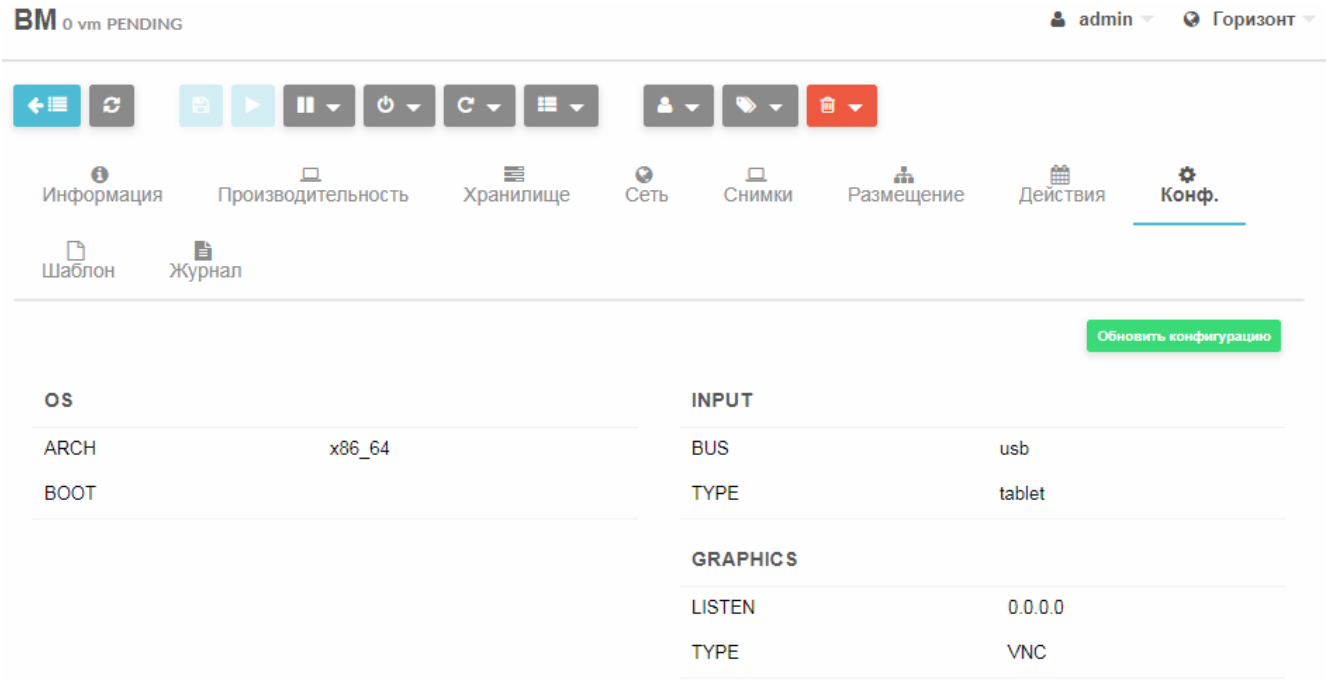


Рисунок 176 - Вкладка "Конфигурация"

При открытии вкладки **Конф.** пользователь увидит информацию о настройках конфигурации ВМ: **OS** – архитектура CPU, **INPUT** – устройство ввода, **GRAPHICS** – графический доступ.

Для изменения конфигурации ВМ необходимо нажать на кнопку **Обновить конфигурацию** (рисунок 176). Откроется мастер настройки изменения конфигурации ВМ (рисунок 177).

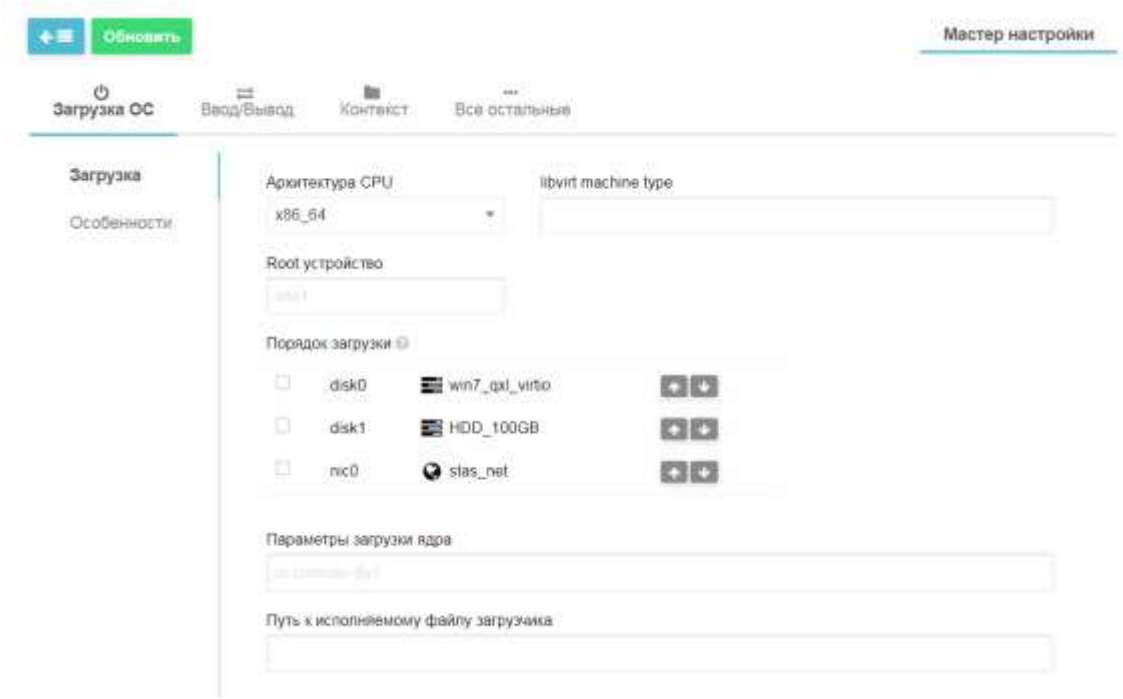


Рисунок 177 - Изменение конфигурации ВМ. Загрузка ОС

На первой вкладке **Загрузка ОС** пользователь может поменять архитектуру CPU и изменить порядок загрузки (рисунок 177).

На вкладке **Ввод/Вывод** пользователь имеет возможность поменять графический доступ и устройства ввода (рисунок 178).

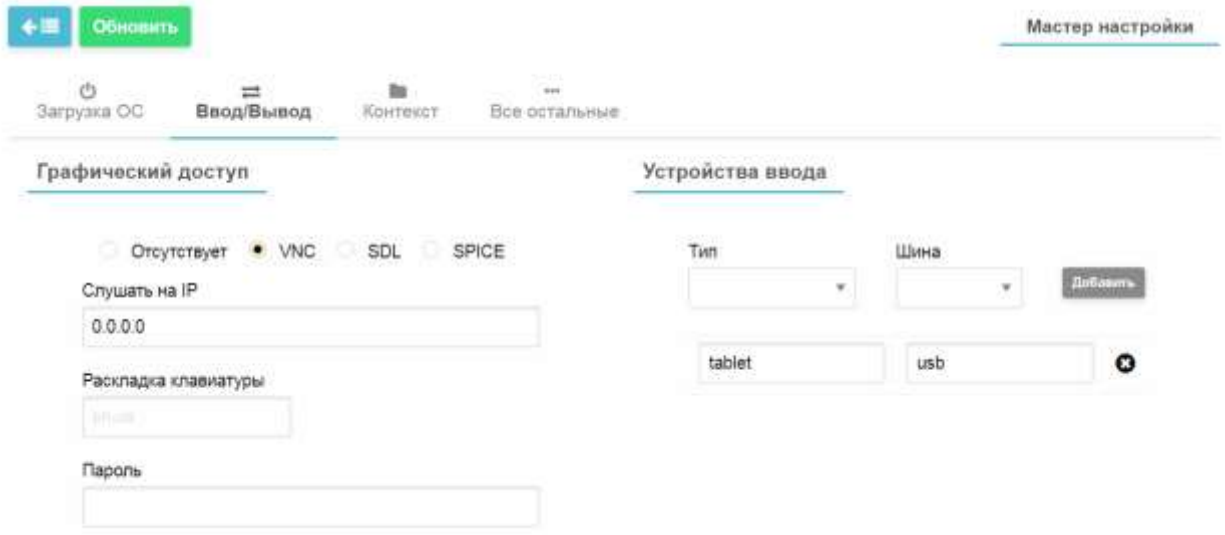


Рисунок 178 - Изменение конфигурации ВМ. Ввод/Вывод

После внесения всех изменений в конфигурацию ВМ необходимо нажать кнопку **Обновить** для обновления и сохранения конфигурации ВМ.

5.18.10 Вкладка “Шаблон”

На вкладке **Шаблон** представлен код шаблона ВМ, на базе которого исполняется ВМ, а также внесенные пользователем в код изменения и коррективы (рисунок 179).

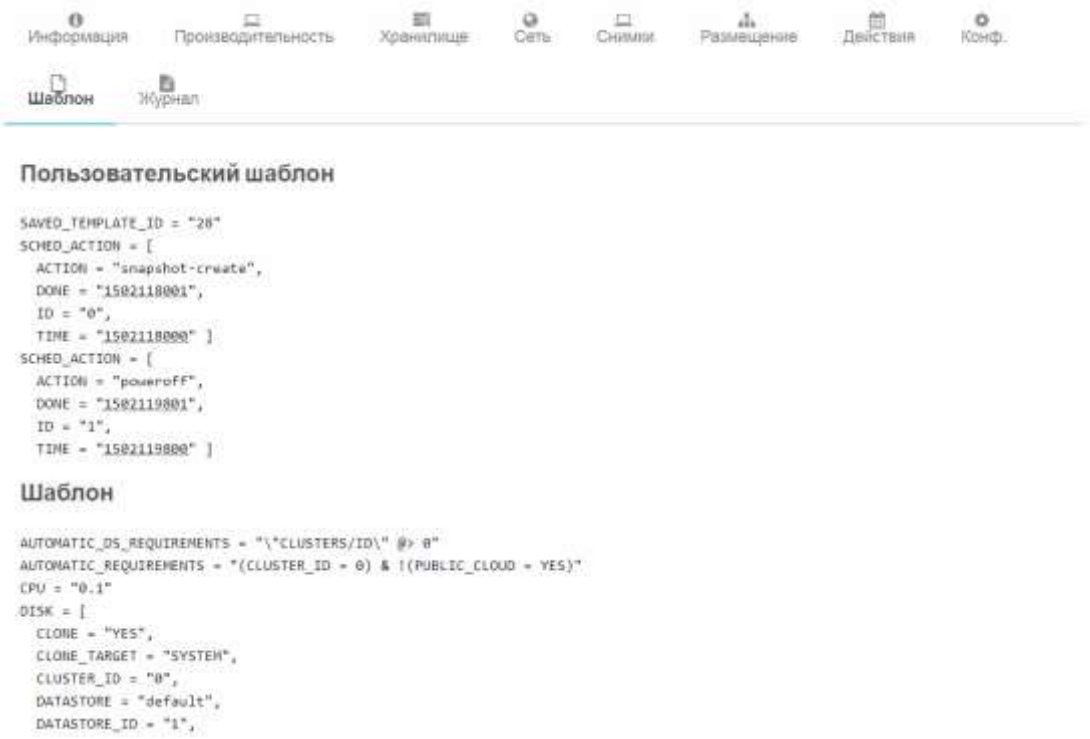


Рисунок 179 - Вкладка "Шаблон"

5.18.11 Вкладка “Журнал”

На вкладке **Журнал** представлена история исполнения ВМ и внесенных изменений в работу ВМ (рисунок 180).

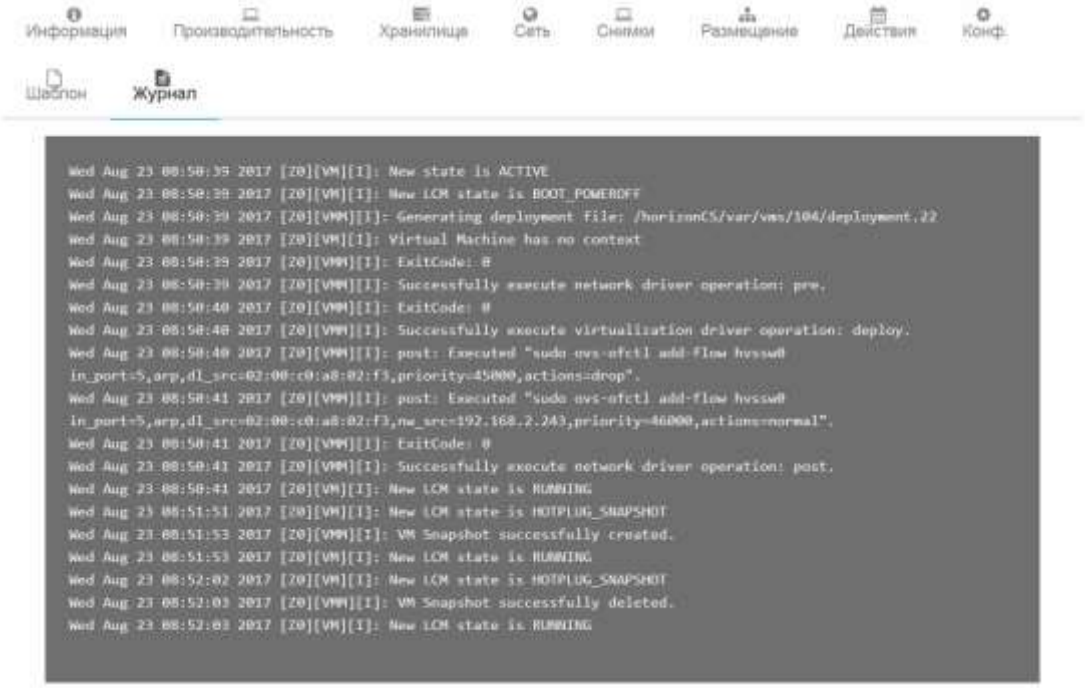


Рисунок 180 – Вкладка "Журнал"

5.19 Создание HA-кластера (кластера высокой доступности)

Кластер – это две или более самостоятельные системы, соединенные в единую систему высокого уровня доступности посредством специального программного и аппаратного обеспечения и представляющие с точки зрения пользователя единый аппаратный или программный ресурс.

Задача создания кластера заключается в обеспечении согласованной работы всех узлов для достижения поставленной цели. Целью может быть высокая устойчивость или доступность (HA, High Availability), высокая вычислительная способность (HP, High Performance), параллельное вычисление, параллельное обслуживание запросов.

Отказоустойчивый кластер (High-Availability, HA) — кластер (группа серверов), спроектированный в соответствии с методиками обеспечения высокой доступности и гарантирующий минимальное время простоя за счёт аппаратной избыточности. Без кластеризации сбой сервера приводит к тому, что поддерживаемые им приложения или сетевые сервисы оказываются недоступны до восстановления его работоспособности. Отказоустойчивая кластеризация исправляет эту ситуацию, перезапуская приложения на других узлах кластера без вмешательства администратора в случае обнаружения аппаратных или программных сбоев. Процесс перезапуска известен как аварийное переключение. В рамках этого процесса программное обеспечение кластеризации может дополнительно настроить узел перед запуском приложения на нём (например, импортировать и смонтировать соответствующие файловые системы, переконфигурировать сетевое оборудование или запустить какие-либо служебные приложения).

Для создания кластера высокой доступности необходимо произвести следующие действия:

1. Подключить общее хранилище – тип «Система», в разделе «Хосты имеющие доступ» IP-адреса серверов виртуализации (минимум два) (см. п. 5.6);
2. Подключить общее хранилище – тип «Файлы», в разделе «Хосты имеющие доступ» IP-адреса серверов виртуализации (минимум два) (см. п. 5.6);
3. Загрузить образ ВМ на общее хранилище (тип «Система») (см. п. 5.7);
4. Создать образ пустого диска на общем хранилище (тип «Файлы») (см. п. 5.8);
5. Создать ВМ из загруженного образа (см. п. 5.16).

Перейти в раздел *Машины→Кластеры ВД*, установить флажок у ВМ, которую планируется запустить в режиме высокой доступности, и нажать кнопку **Создать кластер ВД** (рисунок 181).

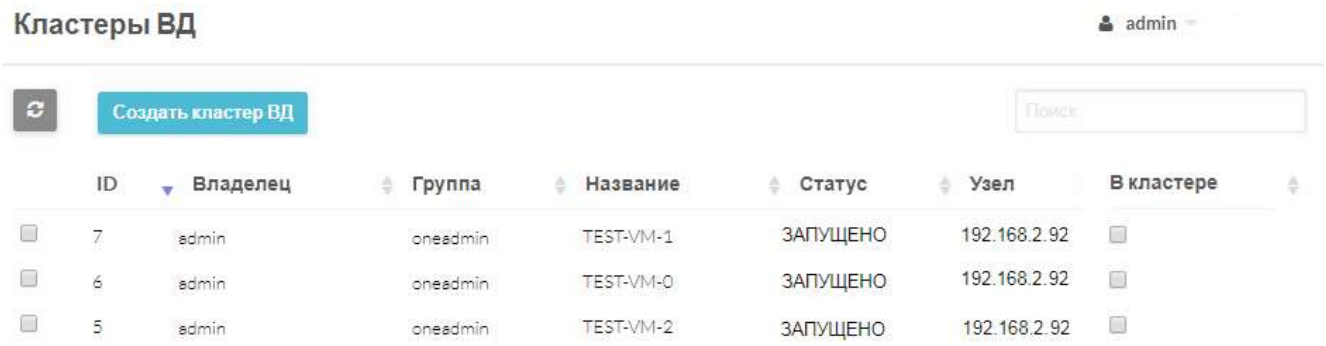


Рисунок 181 - Кластеры НА

После этого откроется окно **Настроить кластер ВД**, в котором следует выделить не менее 2 узлов, на которых сможет работать ВМ в составе кластера, и нажать кнопку **Создать** (рисунок 182).

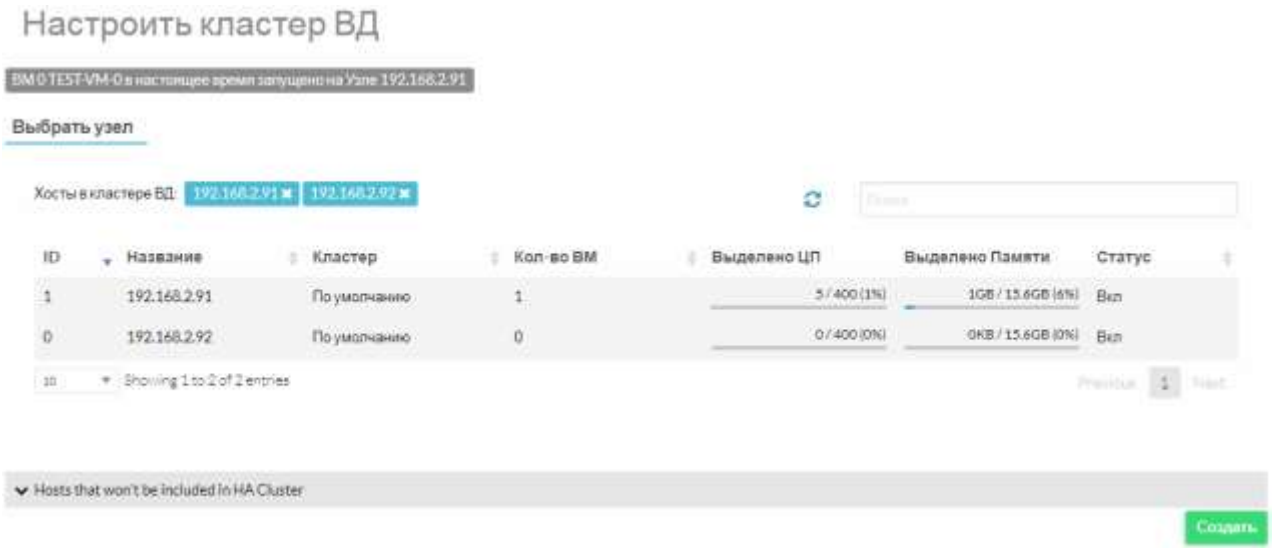


Рисунок 182 - Конфигурирование НА кластера

После окончания конфигурирования кластера в списке ВМ (рисунок 181) напротив настроенной ВМ в столбце **В кластер** появится флажок, подтверждающий перевод ВМ на работу в режиме высокой доступности.

Приложение А

(справочное)

Список сообщений об ошибках, выдаваемых пользователю

В таблице А.1 приведен перечень сообщений об ошибках, выдаваемых пользователю.

Таблица А.1

№ п/п	Сообщение	Пояснения и рекомендации
1	Ошибка подключения к серверу '*IP-адрес сервера*'.	1 По данному IP-адресу отсутствует сервер. 2 Отсутствует подключение терминала к локальной вычислительной сети (ЛВС).
2	Ошибка сервера '*IP-адрес сервера*'. Виртуальная машина '*Название ВМ*' не найдена.	На сервере с данным IP-адресом отсутствует указанная виртуальная машина.
3	Ошибка сервера '*IP-адрес сервера*'. Ошибка конфигурации виртуальной машины '*Название ВМ*'.	1 В настройках конфигурации ВМ произошла ошибка. 2 При настройке ВМ неправильно сконфигурирован графический сервер Spice. Следует настроить Spice согласно настоящему руководству администратора (п. 3.7.8).
4	Ошибка сервера '*IP-адрес сервера*'. Доступ к виртуальной машине '*Название ВМ*' запрещен администратором сервера.	Неправильно настроен графический сервер Spice. Следует настроить Spice согласно настоящему руководству администратора (п. 3.7.8).
5	Ошибка сервера '*IP-адрес сервера*'. Ошибка запуска виртуальной машины '*Название ВМ*'.	Потерян образ виртуальной машины.
6	Неизвестный ключ или неавторизованный пользователь. Компьютер будет отключен.	1 Ошибка в конфигурационном файле.

Перечень принятых сокращений

АРМ	–	автоматизированное рабочее место
ВМ	–	виртуальная машина
ГИС	–	государственная информационная система
ДСП	–	для служебного пользования
К	–	конфиденциально
КП	–	комплекс программ
КС	–	комплект серверный
КТ	–	комплект терминальный
ЛД	–	лазерный диск
НС	–	несекретно
НСД	–	несанкционированный доступ
ОС	–	операционная система
ПИ	–	программное изделие
ПО	–	программное обеспечение
ПРД	–	правила разграничения доступа
ПЭВМ	–	персональная электронная вычислительная машина
РД	–	руководящий документ
СВТ	–	средство вычислительной техники
СГУ	–	система группового управления
СКЗИ	–	средство криптографической защиты информации
СС	–	совершенно секретно
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю России

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					