АО "НТЦ ИТ РОСА"

ПЛАТФОРМА ВИРТУАЛИЗАЦИИ "ROSA VIRTUALIZATION" Версия 3.1

Руководство по установке

РСЮК.10102-02 91 01

Листов 196

2025

Инв. № подл.	Подпись и Дата	Взам.инв.№.	Инв. № дубл.	Подпись и Дата

АННОТАЦИЯ

Данное руководство предназначено для системных администраторов, осуществляющих развертывание, сопровождение и контроль функционирования программного средства "Платформа виртуализации "ROSA Virtualization" (версия 3.1)" РСЮК.10102-02 (далее – ROSA Virtualization).

В руководстве содержатся сведения о процессе, режимах, параметрах установки и первичной настройки ROSA Virtualization.

Дополнительные сведения об администрировании ROSA Virtualization приведены в документе "Платформа виртуализации "ROSA Virtualization" (версия 3.1). Руководство администратора" (шифр – РСЮК.10102-02 92 01).

Сведения о параметрах установки и первичной настройки ROSA Virtualization с развертыванием СУСВ (Система управления средой виртуализации) на выделенном хосте приведены в документе "Платформа виртуализации "ROSA Virtualization" (версия 3.1). Руководство по установке. Развертывание СУСВ на выделенном хосте" (шифр – РСЮК.10102-02 91 02).

Для разработки документа использованы ссылки на следующие стандарты:

– ГОСТ Р 2.105-2019 "Единая система конструкторской документации (ЕСКД). Общие требования к текстовым документам";
– ГОСТ 2.601 "Единая система программной документации. Виды программных документов";
– ГОСТ 19.101-77 "Единая система программной документации. Виды программ и программных документов";
– ГОСТ 19.105-78 "Единая система программной документации. Общие требования к программным документам";
– ГОСТ 19.503-79 Единая система программной документации. Руководство системного программиста".

Настоящий документ подготовлен в соответствии с технологической инструкцией "РОСА. Регламент формирования документации к программным продуктам" (шифр РСЮК.11001-02 90 01).

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение и функции

ROSA Virtualization – платформа виртуализации с интегрированной системой управления, предназначенная для развертывания и эксплуатации виртуального центра обработки данных (ВЦОД) корпоративного уровня.

ROSA Virtualization предоставляет возможности для создания, управления и функционирования свыше тысячи виртуальных машин (ВМ) в одном ВЦОД с применением дискреционной и ролевой модели доступа, а также других встроенных механизмов обеспечения защиты информации (в том числе использование шифрованных виртуальных дисков).

1.2 Область применения

ROSA Virtualization может эксплуатироваться в центрах обработки данных государственных органов и частных организаций различного масштаба.

Версия ROSA Virtualization, сертифицированная ФСТЭК России, может эксплуатироваться в государственных информационных системах, в том числе обрабатывающих персональные данные, в значимых объектах критической информационной инфраструктуры, в автоматизированных системах управления производственными и технологическими процессами, а также в информационных системах общего и специального назначения.

1.3 Архитектура

Программное обеспечение ROSA Virtualization состоит из следующих основных функциональных компонентов:

– гипервизор – компонент устанавливается непосредственно на физический сервер без предустановленной ОС и получает прямой доступ к аппаратному оборудованию этого хоста. Гипервизор обеспечивает создание, запуск и функционирование виртуальных машин на своем хосте;

– система управления средой виртуализации (СУСВ) – в базовой конфигурации компонент располагается во внешнем отказоустойчивом хранилище данных. СУСВ предоставляет графический интерфейс для централизованного управления объектами виртуальной среды (гипервизорами,

хранилищами, кластерами хостов, дата-центрами, виртуальными машинами и т.п.);

– сервер IPA для идентификации и аутентификации доменных пользователей;

– компонент формирования отчетности;

– компонент резервного копирования;

– клиент для ОС семейства Windows с поддержкой версий от XP SP3 и выше;

– дополнительные компоненты – драйверы паравиртуализации, утилиты и служебные программы.

1.4 Режимы функционирования

В зависимости от целей использования существуют различные режимы функционирования ROSA Virtualization. Наиболее распространенными режимами функционирования являются промышленный и тестовый режимы.

1.4.1 Промышленный режим

Промышленный режим функционирования ROSA Virtualization рекомендуется к применению во всех сферах, связанных с обработкой важных данных и работой критичных сервисов организации (например, доменные службы, веб-сервисы, сервисы СУБД, системы документооборота).

В промышленном режиме используются высокопроизводительные модели оборудования, применяется дублирование отдельных узлов аппаратного обеспечения, функционирует система гарантированного питания.

Главным достоинством промышленного режима является повышенная надежность и отказоустойчивость всего вычислительного комплекса, включающая резервирование данных и СУСВ.

К недостаткам промышленного режима функционирования ROSA Virtualization относятся следующие факторы:

– требование к наличию как минимум трех аппаратных серверов промышленных моделей для установки гипервизоров при использовании отказоустойчивой файловой системы GlusterFS или не менее двух при использовании внешнего отказоустойчивого хранилища;

– повышенная нагрузка на сетевую подсистему при использовании распределенных отказоустойчивых файловых систем GlusterFS;

– повышенные требования к вспомогательному оборудованию, включая средства резервирования жестких дисков, а также оборудование сетей, электропитания, охлаждения.

Обеспечение высокой надежности и доступности подразумевает правильную организацию и тщательную настройку не только программной, но и аппаратной части вычислительного комплекса.

1.4.2 Тестовый режим

Тестовый режим функционирования ROSA Virtualization используется для развертывания платформы виртуализации в лабораториях и учебных классах с целью создания стенда для изучения функций и демонстрации возможностей ROSA Virtualization.

В тестовом режиме возможен вариант с использованием одного хоста для установки и функционирования следующих компонентов ROSA Virtualization:

– гипервизор с рабочими ВМ;
– локальное хранилище с развернутой СУСВ.

Тестовый режим не требует проектирования и создания сложных аппаратных и программных конфигураций для сети и хранилищ, а также не предъявляет повышенных требований к аппаратным компонентам как для создаваемой среды виртуализации, так и для иной инфраструктуры вычислительного комплекса.

При этом тестовый режим функционирования ROSA Virtualization не подходит для использования, если в автоматизированной (информационной) системе планируется обрабатывать важные или критичные данные, а также обеспечивать инфраструктуру высоконагруженными и отказоустойчивыми сервисами.

2 УСЛОВИЯ ВЫПОЛНЕНИЯ УСТАНОВКИ

2.1 Требования к аппаратным средствам ROSA Virtualization

В базовой конфигурации установки аппаратное обеспечение ROSA Virtualization должно состоять из следующих технических средств:

– минимум 3 физических сервера с поддержкой функций аппаратной виртуализации, предназначенных для установки и функционирования гипервизоров, при использовании отказоустойчивой файловой системы GlusterFS;

или:

– минимум 2 физических сервера с поддержкой функций аппаратной виртуализации, предназначенных для установки и функционирования гипервизоров, при использовании внешнего отказоустойчивого хранилища;

– сервер каталогов LDAP (возможно использование существующего корпоративного сервера LDAP для идентификации и аутентификации доменных пользователей или сервера IPA, развернутого на ВМ под управлением ROSA Virtualization);

– система хранения данных;

– сетевая инфраструктура высокого уровня производительности.

2.1.1 Требования к серверу для установки гипервизора

Сервер, предназначенный для установки гипервизора, должен соответствовать следующим аппаратным требованиям:

– процессор архитектуры x86_64 с количеством ядер не менее 4 и поддержкой функций аппаратной виртуализации AMD-V (для процессора AMD) или Intel VT (для процессора Intel®). Дополнительно в настройках BIOS / UEFI (в общем случае в разделе "Advanced → CPU Configuration") должен быть включен режим аппаратной виртуализации процессора (установлено значение "Enabled");

– оперативная память – не менее 64 ГБ;

– свободное дисковое пространство – не менее 100 ГБ;

– сетевой интерфейс – не менее 10 Гбит/с – для связи между хостами гипервизоров и системой хранения данных (допускается скорость передачи данных 1 Гбит/с с агрегацией интерфейсов слабонагруженных конфигураций);

– привод DVD / порт USB – для установки ПО.

Поддерживаются следующие модели ЦП:

- AMD:
  - Opteron G4;
  - Opteron G5;
  - EPYC;
- Intel:
  - Nehalem;
  - Westmere;
  - SandyBridge;
  - IvyBridge;
  - Haswell;
  - Broadwell;
  - Skylake Client;
  - Skylake Server;
  - Cascadelake Server.

Для каждой модели ЦП с обновлениями безопасности тип ЦП содержит базовый тип и безопасный тип. Например:

- Семейство серверов Intel Cascadelake;
- Семейство серверов Secure Intel Cascadelake.

Тип безопасного ЦП (Secure CPU) содержит последние обновления.

2.1.2 Требования к серверу для установки сервера каталогов LDAP

Сервер каталогов LDAP (сервер IPA) должен соответствовать следующим аппаратным требованиям:

- процессор архитектуры x86_64 с количеством ядер не менее 2;
- оперативная память – не менее 2 ГБ;
- свободное дисковое пространство – не менее 50 ГБ;
- сетевой интерфейс – не менее 1 Гбит/с;
- привод DVD / порт USB – для установки ПО.

Объем разделяемого хранилища системы хранения данных должен составлять не менее 500 ГБ.

2.2 Требования к межсетевому экрану и используемым портам

2.2.1 Требования к межсетевому экрану для DNS, NTP

ROSA Virtualization не создает DNS- или NTP-сервер, поэтому брандмауэру не нужно иметь открытые порты для входящего трафика.

По умолчанию ROSA Virtualization разрешает исходящий трафик на DNS и NTP на любом адресе назначения. Если вы отключите исходящий трафик, определите исключения для запросов, которые отправляются на DNS и NTP серверы.

Рекомендации и требования:

– СУСВ и все хосты (хост ROSA Virtualization) должны иметь полностью определенное доменное имя и полное, идеально выровненное прямое и обратное разрешение имен.

– Запуск службы DNS как виртуальной машины в среде виртуализации ROSA Virtualization не поддерживается. Все службы DNS, используемые средой виртуализации ROSA Virtualization, должны размещаться вне среды.

– Используйте DNS вместо файла /etc/hosts для разрешения имен. Использование файла hosts обычно требует больше работы и имеет большую вероятность ошибок.

2.2.2 Требования к межсетевому экрану СУСВ

СУСВ требует открытия ряда портов для пропуска сетевого трафика через межсетевой экран системы.

Скрипт настройки движка может автоматически настраивать межсетевой экран.

Описанная в таблице 1 конфигурация межсетевого экрана предполагает конфигурацию по умолчанию.

Таблица 1 – Требования к межсетевому экрану СУСВ

Идентификатор	Порт(ы)	Протокол	Источник	Место назначения	Цель	Зашифровано по умолчанию
M1	-	ICMP	Хосты виртуализации	СУСВ	Необязательный Может помочь в диагностике	Нет
M2	22	TCP	Системы,	СУСВ	Доступ через	Да

Идентификатор	Порт(ы)	Протокол	Источник	Место назначения	Цель	Зашифровано по умолчанию
			используемые для обслуживания СУСВ, включая настройку бэкенда и обновления программного обеспечения		защищенную оболочку (SSH). Необязательный	
M3	2222	TCP	Клиенты, получающие доступ к последовательным консолям виртуальных машин	СУСВ	Доступ по протоколу Secure Shell (SSH) для подключения к последовательным консолям виртуальных машин	Да
M4	80, 443	TCP	Клиенты портала администрирования Клиенты портала ВМ Хосты виртуализации Хосты Linux Клиенты REST API	СУСВ	Предоставляет HTTP (порт 80, не зашифрован) и HTTPS (порт 443, зашифрован) доступ к СУСВ. HTTP перенаправляет соединения на HTTPS	Да
M5	6100	TCP	Клиенты портала администрирования Клиенты портала ВМ	СУСВ	Предоставляет доступ к прокси-серверу веб-сокета для клиента веб-консоли noVNC, когда прокси-сервер веб-сокета запущен на СУСВ	Нет
M6	7410	UDP	Хосты виртуализации Хосты Linux	СУСВ	Если Kdump включен на хостах, откройте этот порт для прослушивателя	Нет

Идентификатор	Порт(ы)	Протокол	Источник	Место назначения	Цель	Зашифровано по умолчанию
					fence_kdump в СУСВ. fence_kdump не предоставляет способа шифрования соединения. Однако вы можете вручную настроить этот порт, чтобы заблокировать доступ с хостов, которые не имеют на это права	
M7	54323	TCP	Клиенты портала администрирования	СУСВ (служба ovirt-imageio)	Требуется для связи со службой ovirt-imageo	Да
M8	6642	TCP	Хосты виртуализации Хосты Linux	База данных Open Virtual Network (OVN)	Подключиться к базе данных Open Virtual Network (OVN)	Да
M9	9696	TCP	Клиенты внешнего сетевого провайдера для OVN	Внешний сетевой провайдер для OVN	Сетевой API OpenStack	Да, с конфигурацией, созданной с помощью engine-setup
M10	35357	TCP	Клиенты внешнего сетевого провайдера для OVN	Внешний сетевой провайдер для OVN	API идентификации OpenStack	Да, с конфигурацией, созданной с помощью engine-setup

Идентификатор	Порт (ы)	Протокол	Источник	Место назначения	Цель	Зашифровано по умолчанию
M11	53	TCP, UDP	СУСВ	DNS-сервер	Запросы поиска DNS с портов выше 1023 до порта 53 и ответы. Открыто по умолчанию	Нет
M12	123	UDP	СУСВ	NTP-сервер	Запросы NTP с портов выше 1023 на порт 123 и ответы. Открыто по умолчанию	Нет

Примечание – Порт для базы данных OVN Northbound (6641) не указан, поскольку в конфигурации по умолчанию единственным клиентом для базы данных OVN Northbound (6641) является ovirt-provider-ovn. Поскольку они оба работают на одном хосте, их связь не видна сети.

По умолчанию ROSA Linux разрешает исходящий трафик на DNS и NTP на любом адресе назначения. Если вы отключите исходящий трафик, сделайте исключения для СУСВ, чтобы он отправлял запросы на DNS- и NTP-серверы. Другие узлы также могут требовать DNS и NTP. В этом случае ознакомьтесь с требованиями для этих узлов и настройте межсетевой экран соответствующим образом.

2.2.3 Требования к межсетевому экрану хоста виртуализации

Хосты ROSA Linux и хосты виртуализации требуют открытия ряда портов для пропуска сетевого трафика через системный межсетевой экран. Правила межсетевого экрана автоматически настраиваются по умолчанию при добавлении нового хоста в СУСВ, перезаписывая любую существующую конфигурацию межсетевого экрана.

Чтобы отключить автоматическую настройку межсетевого экрана при добавлении нового хоста, снимите флажок "Автоматически настраивать брандмауэр" хоста в разделе "Дополнительные параметры".

Таблица 2 – Требования к межсетевому экрану хоста виртуализации

Идентификатор	**Порт(ы)**	**Протокол**	**Источник**	**Место назначения**	**Цель**	**Зашифровано по умолчанию**
H1	22	TCP	СУСВ	Хосты виртуализации	Доступ через защищенную оболочку (SSH). Необязательный	Да
H2	2223	TCP	СУСВ	Хосты виртуализации Хосты ROSA Linux	Доступ по протоколу Secure Shell (SSH) для подключения к последовательным консолям виртуальных машин	Да
H3	161	UDP	Хосты виртуализации Хосты ROSA Linux	СУСВ	Простой протокол управления сетью (SNMP). Требуется только в том случае, если вы хотите, чтобы ловушки простого протокола управления сетью отправлялись с хоста одному или нескольким внешним менеджерам SNMP. Необязательный	Нет
H4	111	TCP	NFS-сервер хранения	Хосты виртуализации Хосты ROSA Linux	NFS-подключения. Необязательный	Нет
H5	5900 - 6923	TCP	Клиенты портала администрир	Хосты виртуализации	Удаленный гостевой доступ к консоли через VNC	Да (необязате

Идентификатор	Порт(ы)	Протокол	Источник	Место назначения	Цель	Зашифровано по умолчанию
			ования Клиенты портала ВМ	Хосты ROSA Linux	и SPICE. Эти порты должны быть открыты для облегчения доступа клиентов к виртуальным машинам	льно)
H6	5989	TCP, UDP	Менеджер объектов общей информационной модели (CIMOM)	Хосты виртуализации Хосты ROSA Linux	Используется Common Information Model Object Managers (CIMOM) для мониторинга виртуальных машин, работающих на хосте. Требуется только в том случае, если вы хотите использовать CIMOM для мониторинга виртуальных машин в вашей среде виртуализации. Необязательный	Нет
H7	9090	TCP	СУСВ Клиентские машины	Хосты виртуализации Хосты ROSA Linux	Требуется для доступа к веб-интерфейсу Cockpit, если он установлен	Да
H8	16514	TCP	Хосты виртуализации Хосты ROSA	Хосты виртуализации Хосты ROSA Linux	Миграция виртуальной машины с использованием	Да

Идентификатор	Порт(ы)	Протокол	Источник	Место назначения	Цель	Зашифровано по умолчанию
			Linux		libvirt	
H9	49152 - 49215	TCP	Хосты виртуализации Хосты ROSA Linux	Хосты виртуализации Хосты ROSA Linux	Миграция и ограждение виртуальных машин с использованием VDSM. Эти порты должны быть открыты для облегчения как автоматизированной, так и ручной миграции виртуальных машин	Да. В зависимости от агента ограждения, миграция осуществляется через libvirt
H10	54321	TCP	СУСВ Хосты виртуализации Хосты ROSA Linux	Хосты виртуализации Хосты ROSA Linux	Связь VDSM с Менеджером и другими хостами виртуализации	Да
H11	54322	TCP	СУСВ служба ovirt -imageio	Хосты виртуализации Хосты ROSA Linux	Требуется для связи со службой ovirt-imageo	Да
H12	6081	UDP	Хосты виртуализации Хосты ROSA Linux	Хосты виртуализации Хосты ROSA Linux	Требуется, когда в качестве сетевого провайдера используется открытая виртуальная сеть (OVN), чтобы разрешить OVN создавать туннели между хостами	Нет

Идентификатор	Порт(ы)	Протокол	Источник	Место назначения	Цель	Зашифровано по умолчанию
H13	53	TCP, UDP	Хосты виртуализации Хосты ROSA Linux	DNS-сервер	Запросы поиска DNS с портов выше 1023 на порт 53 и ответы. Этот порт является обязательным и открыт по умолчанию	Нет
H14	123	UDP	Хосты виртуализации Хосты ROSA Linux	NTP-сервер	Запросы NTP с портов выше 1023 на порт 123 и ответы. Этот порт обязателен и открыт по умолчанию	
H15	4500	TCP, UDP	Хосты виртуализации	Хосты виртуализации	Протокол безопасности Интернета (IPSec)	Да
H16	500	UDP	Хосты виртуализации	Хосты виртуализации	Протокол безопасности Интернета (IPSec)	Да
H17	-	AH, ESP	Хосты виртуализации	Хосты виртуализации	Протокол безопасности Интернета (IPSec)	Да

По умолчанию ROSA Linux разрешает исходящий трафик на DNS и NTP на любом адресе назначения. Если вы отключите исходящий трафик, сделайте исключения для хостов виртуализации.

Хосты ROSA Linux отправляют запросы на DNS- и NTP-серверы. Другие узлы также могут требовать DNS и NTP. В этом случае ознакомьтесь с требованиями для этих узлов и настройте межсетевой экран соответствующим образом.

2.2.4 Требования к межсетевому экрану сервера базы данных

ROSA Virtualization поддерживает использование удаленного сервера базы данных для базы данных СУСВ (engine) и базы данных Data Warehouse (ovirt-engine-history). Если вы планируете использовать удаленный сервер базы данных, он должен разрешать соединения из СУСВ и службы Data Warehouse (которая может быть отдельной от СУСВ).

Аналогично, если вы планируете получить доступ к локальной или удаленной базе данных хранилища данных из внешней системы, база данных должна разрешать подключения из этой системы.

Доступ к базе данных СУСВ из внешних систем не поддерживается.

Таблица 3 – Требования к межсетевому экрану сервера базы данных

Идентификатор	Порт(ы)	Протокол	Источник	Место назначения	Цель	Зашифровано по умолчанию
Д1	5432	TCP, UDP	СУСВ Служба хранилища данных	СУСВ (engine) сервера базы данных Сервер базы данных хранилища данных (ovirt-engine-history)	Порт по умолчанию для подключений к базе данных PostgreSQL	Нет, но может быть включено
Д2	5432	TCP, UDP	Внешние системы	Сервер базы данных хранилища данных (ovirt-engine-history)	Порт по умолчанию для подключений к базе данных PostgreSQL	По умолчанию отключено. Нет, но может быть включено

2.3 Требования к персоналу

Системный администратор, осуществляющий процесс установки и первичной настройки ROSA Virtualization, должен обладать опытом развертывания и сопровождения серверных версий ОС Linux, совместимых с диалектом Red Hat® Enterprise Linux, таких как ROSA "Cobalt" Server, CentOS и т.п.

3 УСТАНОВКА ROSA VIRTUALIZATION

Установка ROSA Virtualization осуществляется администратором в соответствии с заранее выбранной конфигурацией установки – стартовой или базовой.

3.1 Конфигурация установки ROSA Virtualization

3.1.1 Стартовая конфигурация

Стартовая конфигурация установки предназначена для дальнейшего использования ROSA Virtualization в тестовом режиме функционирования в качестве стенда для изучения функций и демонстрации возможностей ROSA Virtualization.

Для установки ROSA Virtualization в стартовой конфигурации выполните следующие действия:

1) установка гипервизора и настройка системных параметров на хосте;

2) подготовка системы хранения данных;

3) установка СУСВ;

4) активация лицензии ROSA Virtualization.

3.1.2 Базовая конфигурация

Базовая конфигурация установки предназначена для дальнейшего использования ROSA Virtualization в промышленном режиме функционирования в качестве платформы виртуализации вычислительных центров, связанных с обработкой важных данных и работой критичных сервисов организации.

Для установки ROSA Virtualization в базовой конфигурации выполните следующие действия:

1) установка гипервизоров и настройка системных параметров на нескольких хостах;

2) подготовка системы хранения данных;

3) установка СУСВ;

4) добавление хостов в кластер;

5) активация лицензии ROSA Virtualization;

6) установка сервера IPA в качестве сервера каталогов LDAP для идентификации и аутентификации доменных пользователей и настройка подключения ROSA Virtualization к службе каталогов LDAP сервера IPA.

3.2 Установка гипервизора на физический сервер

Установка гипервизора ROSA Virtualization осуществляется непосредственно на физический сервер без предустановленной ОС.

Для установки гипервизора используется специальная программа Anaconda, которая предоставляет администратору простой и удобный графический интерфейс, а также позволяет изменять размер существующих разделов диска на этапе установки.

Возможны два варианта установки по типу физического носителя образа дистрибутива, в зависимости от имеющегося аппаратного обеспечения:

– установка с DVD-диска дистрибутива;
– установка с ISO-образа дистрибутива, предварительно записанного на USB-накопитель.

3.2.1 Подготовка к установке гипервизора с DVD диска дистрибутива

По умолчанию дистрибутив ROSA Virtualization поставляется на DVD.

При наличии у сервера DVD-привода установка осуществляется с DVD-диска, на который записан дистрибутив ROSA Virtualization.

Установите DVD-диск с записанным на него дистрибутивом в DVD-накопитель и перейдите к процессу установки (см. п. 3.2.3).

3.2.2 Подготовка к установке гипервизора с USB-накопителя

Если DVD-привод в компьютере отсутствует, установку можно осуществить с USB-накопителя объемом не менее 8 ГБ.

Для этого необходимо загрузить ISO-образ дистрибутива из папки с дистрибутивом в сети или предварительно записать образ с дистрибутивом ROSA Virtualization на USB-накопитель, используя DVD-диск с дистрибутивом, любой компьютер с DVD-приводом и свободным USB-портом.

Загруженный из сети ISO-образ дистрибутива необходимо проверить на целостность, используя контрольные суммы.

3.2.2.1 Проверка контрольной суммы ISO-образа

Для проверки контрольной суммы ISO-образа можно использовать файлы с контрольными суммами, находящиеся в папке с дистрибутивом.

Файлы с расширением .sha1, .sha256, .gost12 содержат контрольную сумму и имя файла, для которого была рассчитана контрольная сумма.

Для контроля целостности ISO-образа достаточно проверить любую из указанных контрольных сумм, используя доступные вам инструменты.

3.2.2.1.1 Проверка контрольной суммы SHA256

Для проверки контрольной суммы SHA256 файла myfile.iso, используя контрольную сумму, ранее сохраненную в файле myfile.sha256, выполните следующие шаги в терминале Linux:

1) Убедитесь, что файлы myfile.iso и myile.sha256 загружены и находятся в одной директории.

2) Используйте команду `sha256sum` вместе с опцией "-c", чтобы проверить контрольную сумму. Выполните следующую команду:

```
$ sha256sum -c myfile.sha256
```

Для дистрибутива ROSA Virtualization, выпущенного 12.05.2025 г. (файл RV-3.1-20250512.0-rv-x86_64-dvd1.iso), команда выглядит следующим образом:

```
$ sha256sum -c RV-3.1-20250512.0-rv-x86_64-dvd1.sha256
```

3) Если контрольная сумма совпадает, вы увидите сообщение, подобное этому:

```
  myfile.iso: OK
```

или

```
  myfile.iso: ЦЕЛ
```

в зависимости от локализации консоли (английский/русский язык).

При совпадении контрольной суммы вы можете использовать файл с ISO-образом для установки.

Если контрольная сумма не совпадает, вы получите сообщение об ошибке, и вам необходимо будет загрузить ISO-образ заново и осуществить повторную проверку контрольной суммы.

Пример проверки контрольной суммы в консоли:

```
$ sha256sum -c RV-3.1-20250512.0-rv-x86_64-dvd1.sha256
RV-3.1-20250512.0-rv-x86_64-dvd1.iso: ЦЕЛ
```

Следует обратить внимание, что файл file.sha256 должен иметь формат, который включает имя файла и его контрольную сумму. Например, содержимое файла должно выглядеть так:

```
<контрольная_сумма>  file.iso
```

3.2.2.1.2 Проверка контрольной суммы gost12 с использованием утилиты gost12sum

Для выполнения команд, приведенных в данном разделе, необходимо установить пакет gostsum.

Для установки пакета в семействе ОС CentOS/Fedora/RedHat вы можете использовать команду:

```
$ sudo yum install gostsum
```

Для проверки контрольной суммы GOST12 файла myfile.iso, используя контрольную сумму, ранее сохраненную в файле myfile.gost12, выполните следующие шаги в терминале Linux:

1) Убедитесь, что файлы myfile.iso и myfile.gost12 загружены и находятся в одной директории.

2) Используйте команду `gost12sum`, чтобы подсчитать контрольную сумму. Выполните следующую команду:

```
$ gost12sum myfile.iso
```

Для дистрибутива ROSA Virtualization, выпущенного 12.05.2025 г. (файл RV-3.1-20250512.0-rv-x86_64-dvd1.iso), команда выглядит следующим образом:

```
$ gost12sum RV-3.1-20250512.0-rv-x86_64-dvd1.iso
```

3) Выведите в терминал контрольную сумму, сохраненную в файл myfile.gost12, используя команду `cat`:

```
$ cat myfile.gost12
```

При совпадении контрольной суммы с подсчитанной ранее вы можете использовать файл с ISO-образом для установки.

Если контрольная сумма не совпадает, вам необходимо загрузить ISO-образ заново и осуществить повторную проверку контрольной суммы.

Пример подсчёта контрольной суммы в консоли:

```
    $ gost12sum RV-3.1-20250512.0-rv-x86_64-dvd1.iso
    d9a034774dd1a613760de776e1b8bc8592234114c17a7870921c9e54649a
c2ab RV-3.1-20250512.0-rv-x86_64-dvd1.iso
```

Пример вывода ранее сохранённой контрольной суммы в консоль:

```
    $ cat RV-3.1-20250512.0-rv-x86_64-dvd1.gost12
    d9a034774dd1a613760de776e1b8bc8592234114c17a7870921c9e54649a
c2ab RV-3.1-20250512.0-rv-x86_64-dvd1.iso
```

В данном случае контрольные суммы совпадают, и ISO-образ диска с дистрибутивом может быть использован для установки.

3.2.2.1.3 Проверка контрольной суммы gost12 с использованием утилиты openssl в ROSA Linux

Для выполнения команд, приведенных в данном разделе, необходим компьютер с установленной на нем ОС ROSA Linux или ROSA Virtualization. Вы можете установить на любой компьютер или сервер ROSA Virtualization в минимальной конфигурации или использовать любой хост ROSA Virtualization.

Для проверки наличия необходимой версии операционной системы выполните в консоли команду `hostnamectl` с фильтром по параметру "Operating System":

```
    # hostnamectl | grep "Operating System"
      Operating System: ROSA Virtualization 3.1.0
```

В данном случае на хосте установлена ОС ROSA Virtualization 3.1.0, и он может быть использован для проверки контрольной суммы.

Убедитесь, что у вас установлен пакет OpenSSL:

```
    # yum info openssl | grep "Имя"
    Имя          : openssl
```

Если пакет OpenSSL установлен, то вы можете переходить к следующим шагам.

Для проверки контрольной суммы GOST12 файла myfile.iso, используя контрольную сумму, ранее сохраненную в файле myfile.gost12, выполните следующие шаги в терминале Linux:

1) Убедитесь, что файлы myfile.iso и myfile.gost12 загружены и находятся в одной директории.

2) Используйте команду `openssl`, чтобы подсчитать контрольную сумму. Выполните следующую команду:

```
$ openssl dgst -streebog256 myfile.iso
```

Для дистрибутива ROSA Virtualization, выпущенного 12.05.2025 г. (файл RV-3.1-20250512.0-rv-x86_64-dvd1.iso), команда выглядит следующим образом:

```
$ openssl dgst -streebog256 RV-3.1-20250512.0-rv-x86_64-
dvd1.iso
```

3) Выведите в терминал контрольную сумму, сохраненную в файл, используя команду `cat`:

```
$ cat myfile.gost12
```

При совпадении контрольной суммы с подсчитанной ранее, вы можете использовать файл с ISO-образом для установки.

Если контрольная сумма не совпадает, вам необходимо загрузить ISO-образ заново и осуществить повторную проверку контрольной суммы.

Пример подсчёта контрольной суммы в консоли:

```
$ openssl dgst -streebog256 RV-3.1-20250512.0-rv-x86_64-
dvd1.iso
md_gost12_256(RV-3.1-20250512.0-rv-x86_64-dvd1.iso)=
d9a034774dd1a613760de776e1b8bc8592234114c17a7870921c9e54649ac2ab
```

Контрольная сумма выводится после знака "=".

Пример вывода ранее сохранённой контрольной суммы в консоль:

```
$ cat RV-3.1-20250512.0-rv-x86_64-dvd1.gost12
d9a034774dd1a613760de776e1b8bc8592234114c17a7870921c9e54649a
c2ab RV-3.1-20250512.0-rv-x86_64-dvd1.iso
```

В данном случае контрольные суммы совпадают, и ISO-образ диска с дистрибутивом может быть использован для установки.

3.2.2.2 Запись образа дистрибутива ROSA Virtualization на USB-накопитель в ОС Linux

Для записи образа вставьте диск с дистрибутивом ROSA Virtualization в DVD-привод, подключите USB-накопитель и скопируйте на него содержимое диска.

Примечание – В данном разделе приводятся команды для выполнения копирования диска на USB-накопитель в ОС Linux семейства CentOS / ROSA Server / ROSA Desktop / RedHat. Выполнение команд в других версиях ОС Linux может отличаться. Для копирования содержимого DVD-диска на USB-накопитель в других операционных системах обратитесь к Руководству пользователя вашей операционной системы.

Важно – Для выполнения указанных ниже команд вам нужны права суперпользователя (администратора) системы. Если у вас отсутствуют права на выполнение операций с диском на уровне администратора, обратитесь к администратору вашей системы.

На компьютере с установленной ОС семейства Linux для копирования диска выполните следующую консольную команду с правами суперпользователя (root):

```
# dd if=/dev/sr0 of=/dev/sdX
```

где "X" – буква диска, соответствующая USB-накопителю.

Примечание – Для получения сведений о подключенных к системе накопителях выполните следующую консольную команду с правами суперпользователя root:

```
# fdisk -l
```

При успешном подключении USB-накопителя в консоль будет выведена информация подобного вида:

```
# fdisk -l
Диск /dev/nvme0n1: 60 GiB, 64424509440 байт, 125829120
секторов
Единицы: секторов по 1 * 512 = 512 байт
Размер сектора (логический/физический): 512 байт / 512 байт
Размер I/O (минимальный/оптимальный): 512 байт / 512 байт
Тип метки диска: dos
Идентификатор диска: 0x9ab46fba

Устр-во        Загрузочный  начало     Конец   Секторы
Размер Идентификатор Тип
/dev/nvme0n1p1 *             2048   2099199   2097152
1G           83 Linux
/dev/nvme0n1p2            2099200 125829119 123729920
59G           8e Linux LVM
```

```
     Диск /dev/mapper/rv-root: 15,1 GiB, 16257122304 байт,
31752192 секторов
     Единицы: секторов по 1 * 512 = 512 байт
     Размер сектора (логический/физический): 512 байт / 512 байт
     Размер I/O (минимальный/оптимальный): 65536 байт / 65536
байт

     Диск /dev/mapper/rv-swap: 3,9 GiB, 4215275520 байт, 8232960
секторов
     Единицы: секторов по 1 * 512 = 512 байт
     Размер сектора (логический/физический): 512 байт / 512 байт
     Размер I/O (минимальный/оптимальный): 512 байт / 512 байт


     Диск /dev/mapper/rv-var_log_audit: 2 GiB, 2147483648 байт,
4194304 секторов
     Единицы: секторов по 1 * 512 = 512 байт
     Размер сектора (логический/физический): 512 байт / 512 байт
     Размер I/O (минимальный/оптимальный): 65536 байт / 65536
байт

     Диск /dev/mapper/rv-var_log: 8 GiB, 8589934592 байт,
16777216 секторов
     Единицы: секторов по 1 * 512 = 512 байт
     Размер сектора (логический/физический): 512 байт / 512 байт
     Размер I/O (минимальный/оптимальный): 65536 байт / 65536
байт

     Диск /dev/mapper/rv-var: 15 GiB, 16106127360 байт, 31457280
секторов
     Единицы: секторов по 1 * 512 = 512 байт
     Размер сектора (логический/физический): 512 байт / 512 байт
     Размер I/O (минимальный/оптимальный): 65536 байт / 65536
байт

     Диск /dev/mapper/rv-tmp: 2 GiB, 2147483648 байт, 4194304
секторов
```

```
     Единицы: секторов по 1 * 512 = 512 байт
     Размер сектора (логический/физический): 512 байт / 512 байт
     Размер I/O (минимальный/оптимальный): 65536 байт / 65536
байт


     Диск /dev/mapper/rv-home: 1 GiB, 1073741824 байт, 2097152
секторов
     Единицы: секторов по 1 * 512 = 512 байт
     Размер сектора (логический/физический): 512 байт / 512 байт
     Размер I/O (минимальный/оптимальный): 65536 байт / 65536
байт


     Диск /dev/sda: 3,8 GiB, 4026531840 байт, 7864320 секторов
     Единицы: секторов по 1 * 512 = 512 байт
     Размер сектора (логический/физический): 512 байт / 512 байт
     Размер I/O (минимальный/оптимальный): 512 байт / 512 байт
     Тип метки диска: dos
     Идентификатор диска: 0x0060d108

     Устр-во    Загрузочный начало   Конец Секторы Размер
Идентификатор Тип
     /dev/sda1  *            2048 7864319 7862272   3,8G
e W95 FAT16 (LBA)
```

Раздел /dev/sda1 с файловой системой W95 FAT16 (LBA) соответствует подключенному к компьютеру USB-накопителю.

Для вывода информации только о подключенных к системе накопителях можно воспользоваться командой `fdisk -l | grep sda`:

```
     # fdisk -l | grep sda
     Диск /dev/sda: 3,8 GiB, 4026531840 байт, 7864320 секторов
     /dev/sda1  *            2048 7864319 7862272   3,8G
e W95 FAT16 (LBA)
```

Раздел /dev/sda1 соответствует первому подключенному к системе накопителю. При использовании нескольких накопителей они могут быть идентифицированы как /dev/sdb1, /dev/sdc1 и т.д.

3.2.3 Запуск программы установки

Для установки гипервизора загрузите сервер с носителя с дистрибутивом ROSA Virtualization.

Важно – В настройках BIOS/UEFI установите приоритет загрузки сервера с DVD- или USB-накопителя, а также включите режим аппаратной виртуализации процессора.

В процессе загрузки сервера на экране автоматически появится меню, позволяющее запускать программу установки гипервизора в различных режимах (рисунок 1).

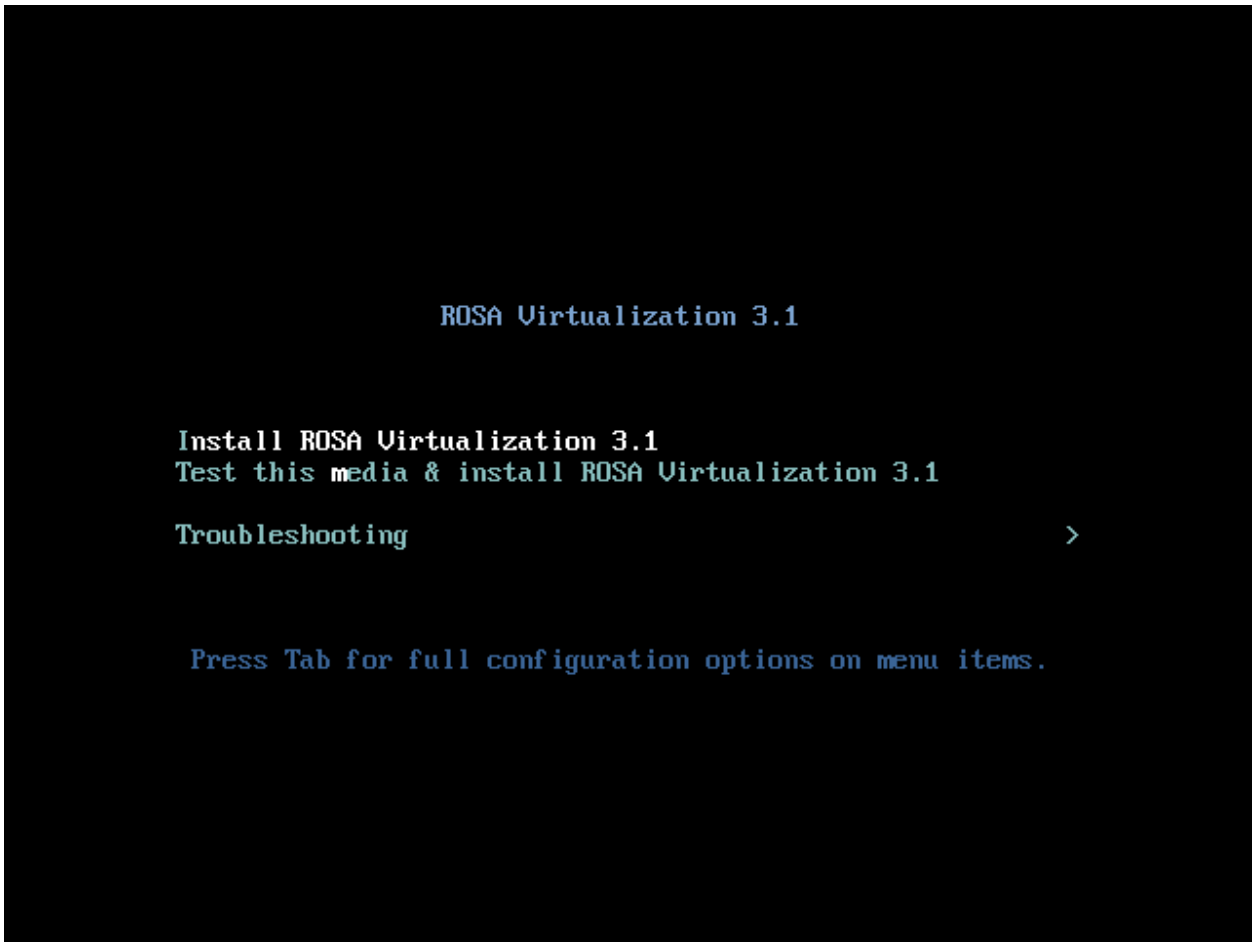

Рисунок 1 – Меню установки ROSA Virtualization 3.1

Для запуска графического интерфейса программы установки гипервизора нажмите клавишу `Enter` или дождитесь автоматического старта установки через 60 секунд.

Примечания

1) В данном руководстве рассматривается вариант установки гипервизора с использованием графического интерфейса программы Anaconda, но в редких случаях (например, когда программа установки не может корректно определить видеокарту) может потребоваться консольный режим установки гипервизора в текстовом интерфейсе программы Anaconda.

2) В текстовом режиме установки гипервизора будут доступны только стандартные схемы разбиения диска на разделы (например, можно использовать весь диск или удалить существующие разделы, но нельзя добавлять разделы и файловые системы).

3) Для запуска текстового интерфейса программы установки гипервизора нажмите клавишу `Tab`, затем введите через пробел слово "text" в конец строки с параметрами загрузки и нажмите клавишу `Enter`.

3.2.3.1 Выбор языка для установки

После запуска программы установки на экране появится окно приветствия (рисунок 2), предназначенное для выбора языка интерфейса, который будет использоваться в процессе установки гипервизора.

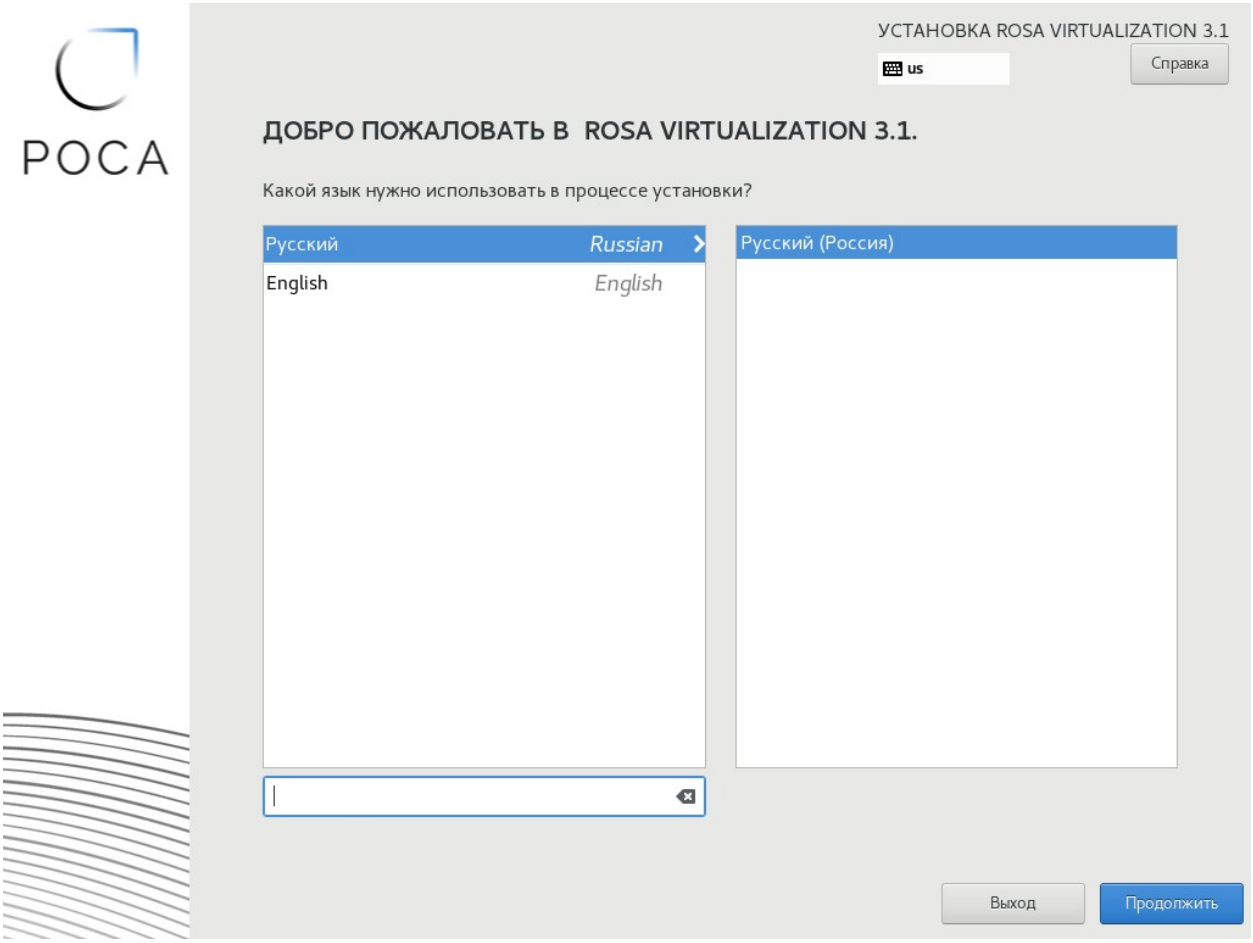

Рисунок 2 – Окно приветствия программы установки

Используя полосу прокрутки и строку поиска выберите из списка в левой области окна необходимый язык интерфейса установки, а в правой области – языковой регион.

По умолчанию язык интерфейса установки – "Русский (Россия)".

Для перехода к следующему этапу установки нажмите кнопку Продолжить.

3.2.4 Параметры установки

3.2.4.1 Настройка параметров установки системы

На экране появится интерфейс, предназначенный для обзора и последующей настройки параметров установки. Вместо последовательного определения параметров программа установки дает возможность настроить

параметры в произвольном порядке, выбирая необходимые секции с требуемыми параметрами в меню "Сводка установки" (рисунок 3).

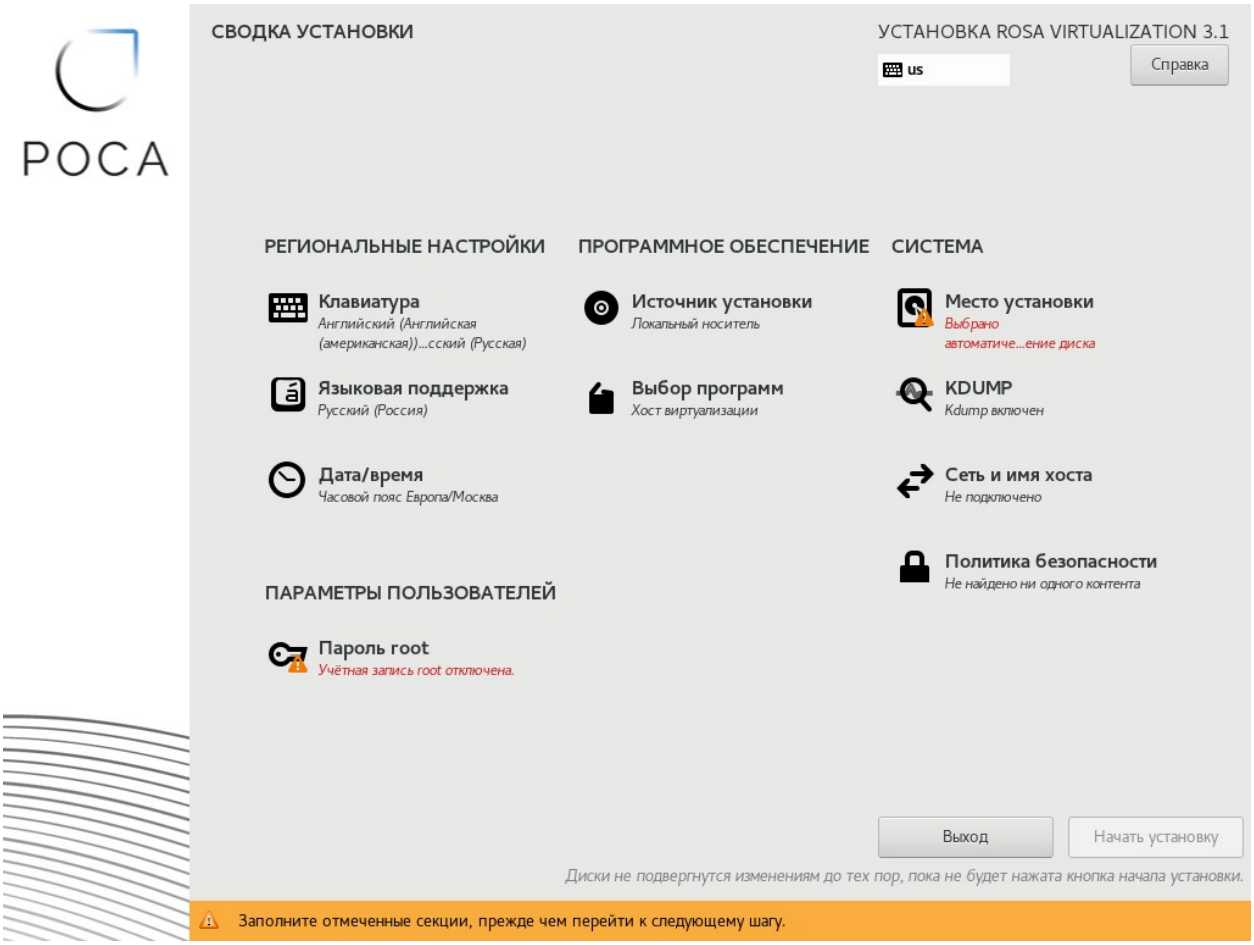

Рисунок 3 – Сводка установки

В меню "Сводка установки" параметры установки распределены по следующим разделам – "Региональные настройки", "Программное обеспечение", "Система", "Параметры пользователей".

3.2.4.2 Региональные настройки

Раздел "Региональные настройки" содержит следующие секции с параметрами установки:

– Клавиатура – интерфейс секции позволяет выбрать раскладку клавиатуры и указать комбинацию клавиш для переключения раскладки. Значения параметров по умолчанию – раскладка "Английская/Русская" с комбинацией клавиш `Alt`+`Shift` для переключения раскладки;

– Языковая поддержка – интерфейс секции предназначен для добавления дополнительных языков в пользовательский интерфейс гипервизора. Значение параметра по умолчанию – "Русский (Россия)";

– Дата/время – интерфейс секции предназначен для проверки и при необходимости корректировки автоматически определенных даты, времени и часового пояса, а также для подключения гипервизора к внешним сетевым источникам точного времени по протоколу NTP.

3.2.4.3 Настройка устанавливаемого программного обеспечения

Раздел "Программное обеспечение" содержит следующие секции с параметрами установки:

– Источник установки – интерфейс секции позволяет указать расположение установочных файлов (локальный носитель или сетевой репозиторий) и осуществить проверку целостности установочного носителя. Если программа установки гипервизора была запущена с DVD- или USB-накопителя, то установочный носитель будет обнаружен автоматически;

– Выбор программ – интерфейс секции предназначен для выбора базового программного окружения, которое будет установлено в процессе инсталляции ПО.

Примечание – Значение параметра по умолчанию – "Хост виртуализации" (функции гипервизора).

3.2.4.3.1 Выбор типа устанавливаемого программного обеспечения

Выбрать тип устанавливаемых компонент можно в меню "Выбор программ" (рисунок 4).

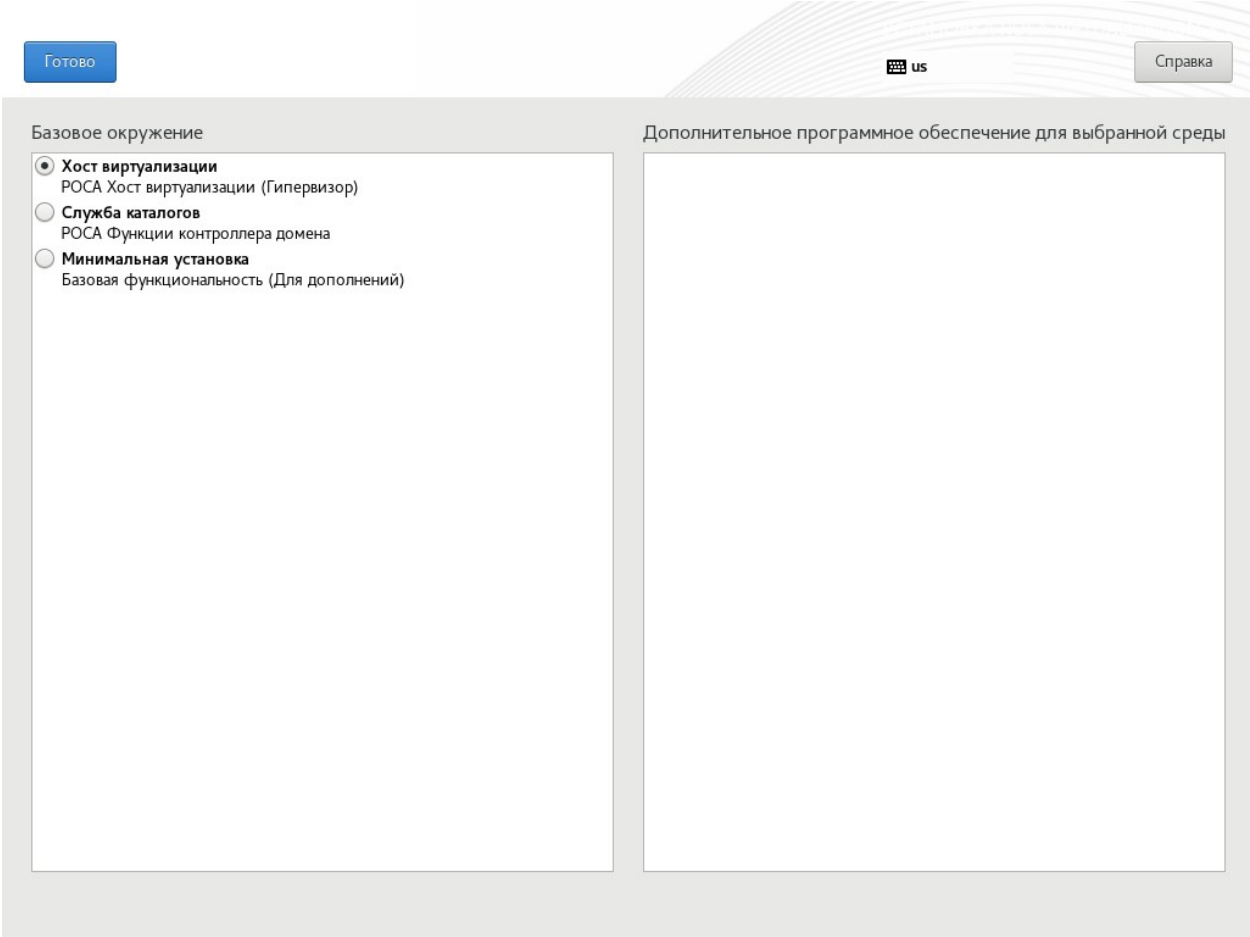

Рисунок 4 – Выбор типа устанавливаемого ПО (выбран Хост виртуализации)

Доступны следующие компоненты базового окружения:

– Хост виртуализации – выберите данную опцию для установки хоста виртуализации (функции гипервизора).

– Служба каталогов – выберите данную опцию для установки службы каталогов/контроллера домена.

– Минимальная установка – выберите данную опцию для установки минимальной конфигурации сервера.

После выбора необходимого компонента нажмите на кнопку Готово для возврата на экранную форму "Сводка установки".

3.2.4.4 Настройка параметров системы. Сетевые настройки. Выбор имени хоста

Раздел "Система" содержит следующие секции с параметрами установки:

– Место установки – интерфейс секции предназначен для выбора диска для установки гипервизора и настройки конфигурации разделов диска в автоматическом или ручном режиме;

– KDUMP – интерфейс секции предназначен для управления (включение/выключение) и настройки резервирования памяти для kdump (механизм сбора статистики о сбоях ядра). Значение параметра по умолчанию – "kdump включен с резервированием памяти в автоматическом режиме";

– Сеть и имя хоста – интерфейс секции предназначен для настройки параметров сетевых адаптеров и указания имени хоста гипервизора;

Раздел "Параметры пользователей" содержит секцию "Пароль root", которая предназначена для установки пароля учетной записи суперпользователя root (администратора гипервизора).

Под наименованием каждой секции приводится информация о текущих параметрах, настроенных автоматически программой установки.

Важно – Секции, отмеченные восклицательным знаком, являются обязательными для настройки параметров, что также подтверждает сообщение в нижней части окна, выделенное оранжевым фоном – "Заполните отмеченные секции, прежде чем перейти к следующему шагу".

Нажмите на наименование секции для перехода к интерфейсу настройки соответствующих параметров.

Важно – Следующие секции являются обязательными или рекомендуемыми для настройки параметров установки гипервизора:

– Дата/время (см. пункт 3.2.4.5);
– Целевое устройство установки (см. пункт 3.2.4.6);
– Сеть и имя хоста (см. пункт 3.2.4.7);
– Пароль root (см. пункт 3.2.4.8).

Примечание – Настройка "Даты/времени" с использованием серверов NTP требует подключения к внешним сетевым источникам точного времени. Настройте "Сеть и имя хоста" до начала настройки "Даты/времени", если вы планируете использовать внешние сетевые источники точного времени.

После настройки всех обязательных и рекомендуемых параметров нажмите кнопку Начать установку для старта процесса установки гипервизора (см. пункт 3.2.5).

Для отмены установки нажмите кнопку Выход и подтвердите прекращение процесса установки.

3.2.4.5 Дата, время и часовой пояс

Интерфейс секции "Дата/время" предназначен для проверки и при необходимости корректировки автоматически определенных даты, времени и часового пояса, а также для подключения гипервизора к внешним сетевым источникам точного времени по протоколу NTP (рисунок 5).

Важно – Для настройка "Даты/времени" с использованием серверов NTP требуется настроенное сетевое подключение (настройка осуществляется в секции "Сеть и имя хоста"), обеспечивающее сетевую доступность серверов NTP.

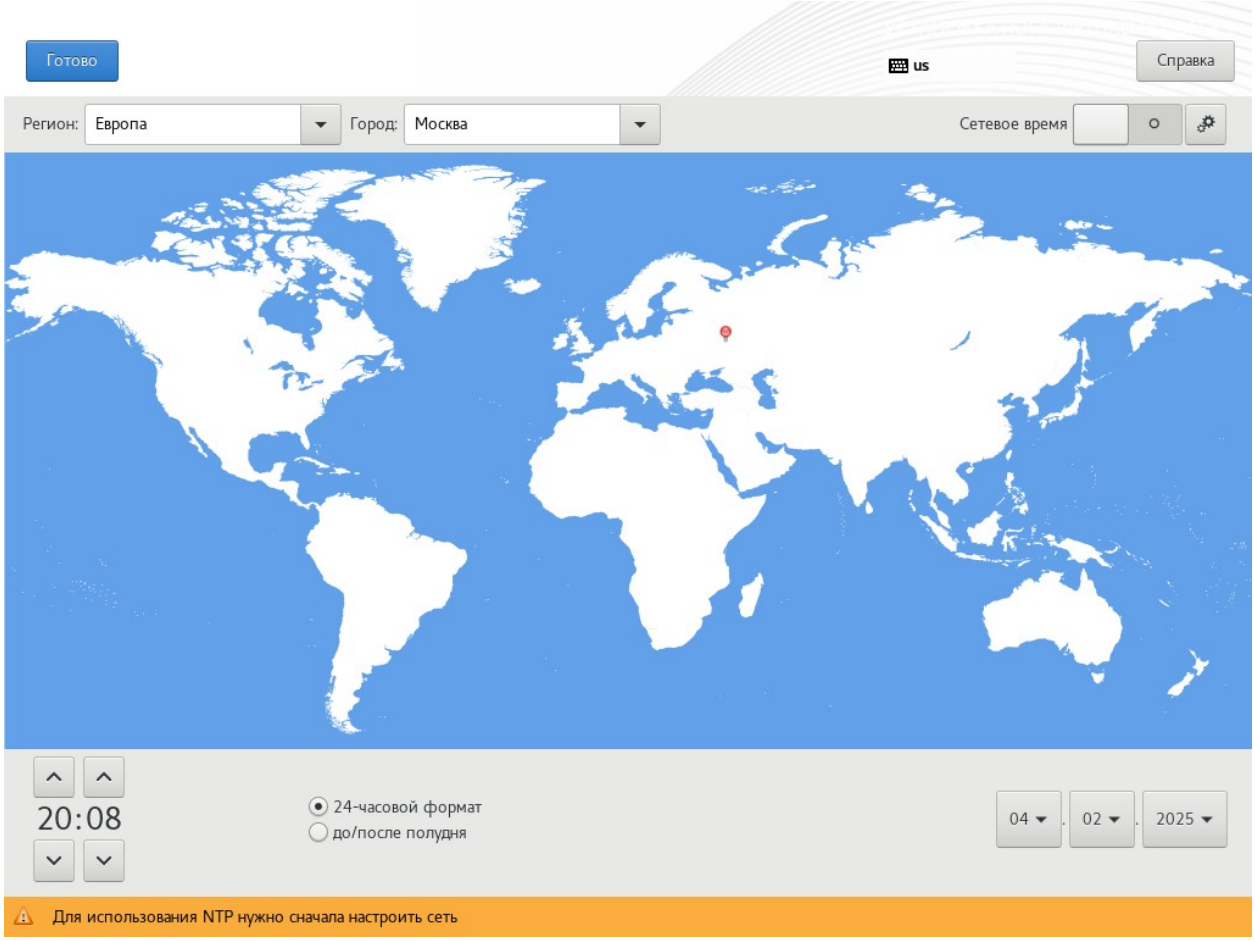

Рисунок 5 – Настройка даты, времени и часового пояса

Для настройки времени и часового пояса выберите последовательно регион и город из соответствующих выпадающих списков. Если необходимого города нет в списке, выберите ближайший город в той же часовой зоне.

Важно – Настройте часовой пояс, даже если вы планируете использовать протокол NTP для синхронизации часов.

Если системные часы показывают неверное время, откорректируйте его с помощью кнопок ∧ (больше) и ∨ (меньше). Для выбора формата отображения времени установите в соответствующее положение переключатель – 24-часовой формат или "AM/PM".

При необходимости скорректируйте дату. Для этого выберите из выпадающих списков текущие значения дня, месяца и года.

Важно – Для использования внешних сетевых источников точного времени по протоколу NTP необходимо сначала настроить сетевое подключение, обеспечив сетевую доступность серверов NTP.

3.2.4.5.1 Настройка сетевого времени с использованием протокола NTP

Если сервер подключен к сети, будет доступен переключатель "Сетевое время". Чтобы включить синхронизацию часов с использованием протокола NTP, установите во включенное положение переключатель "Сетевое время".

Для настройки синхронизации времени с определенным сервером NTP нажмите кнопку конфигурации . На экране появится модальное окно "Добавить и отметить используемые серверы NTP" (рисунок 6).

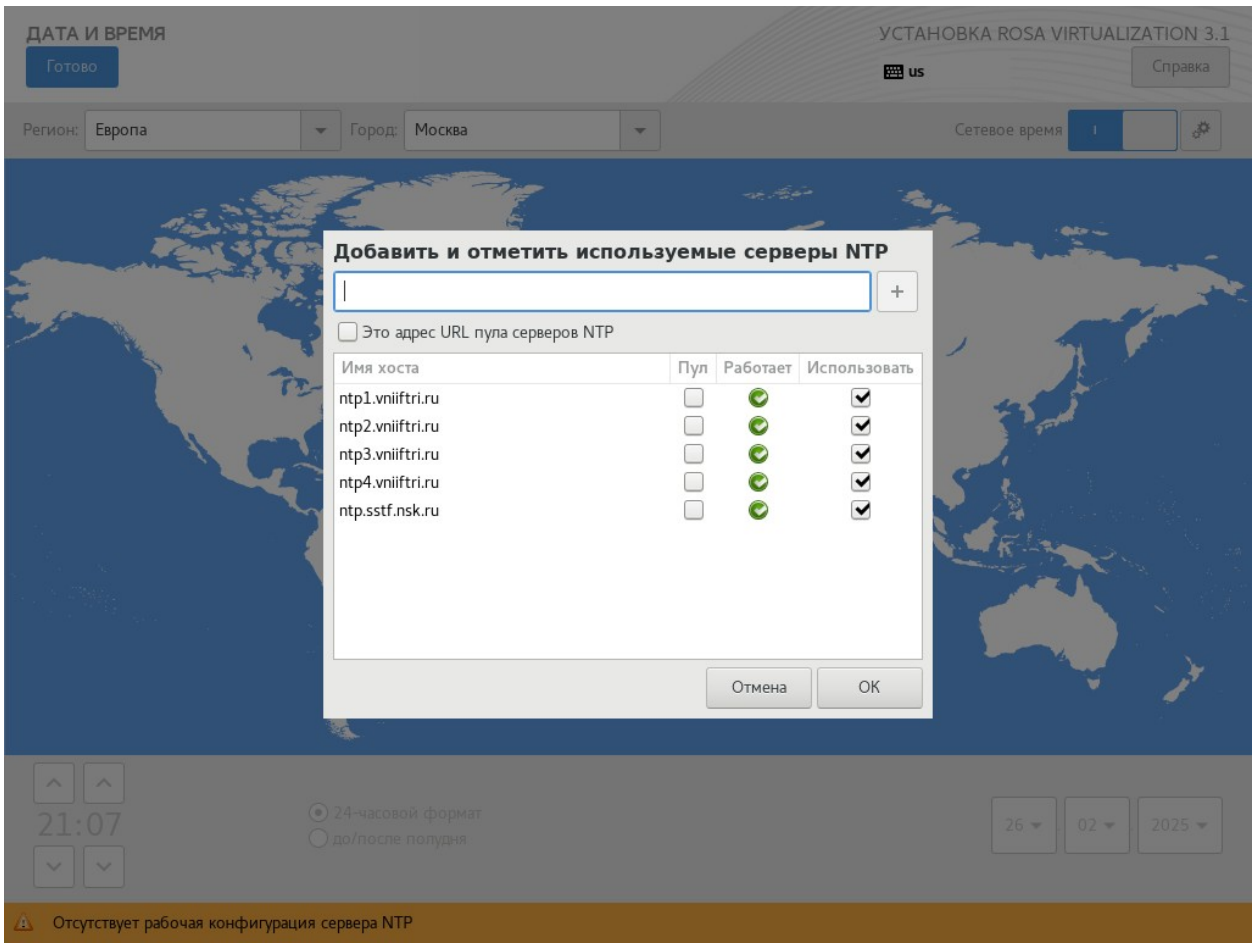

Рисунок 6 – Выбор серверов NTP

В модальном окне отобразится список используемых (предварительно настроенных) серверов NTP.

Для выбора сервера NTP из списка установите флажок "Использовать".

Для добавления дополнительного сервера NTP в список введите имя узла (адрес) и нажмите кнопку +. Для завершения настройки нажмите кнопку OK (Рисунок 6).

Примечание – Если во время установки выбранный сервер NTP недоступен, системное время будет выставлено, когда сервер NTP станет активным.

После настройки параметров даты и времени нажмите кнопку Готово для возвращения в меню "Сводка установки".

3.2.4.6 Выбор места установки

Интерфейс секции "Целевое устройство установки" предназначен для выбора диска для установки гипервизора и настройки конфигурации разделов диска в автоматическом или ручном режиме (рисунок 7).

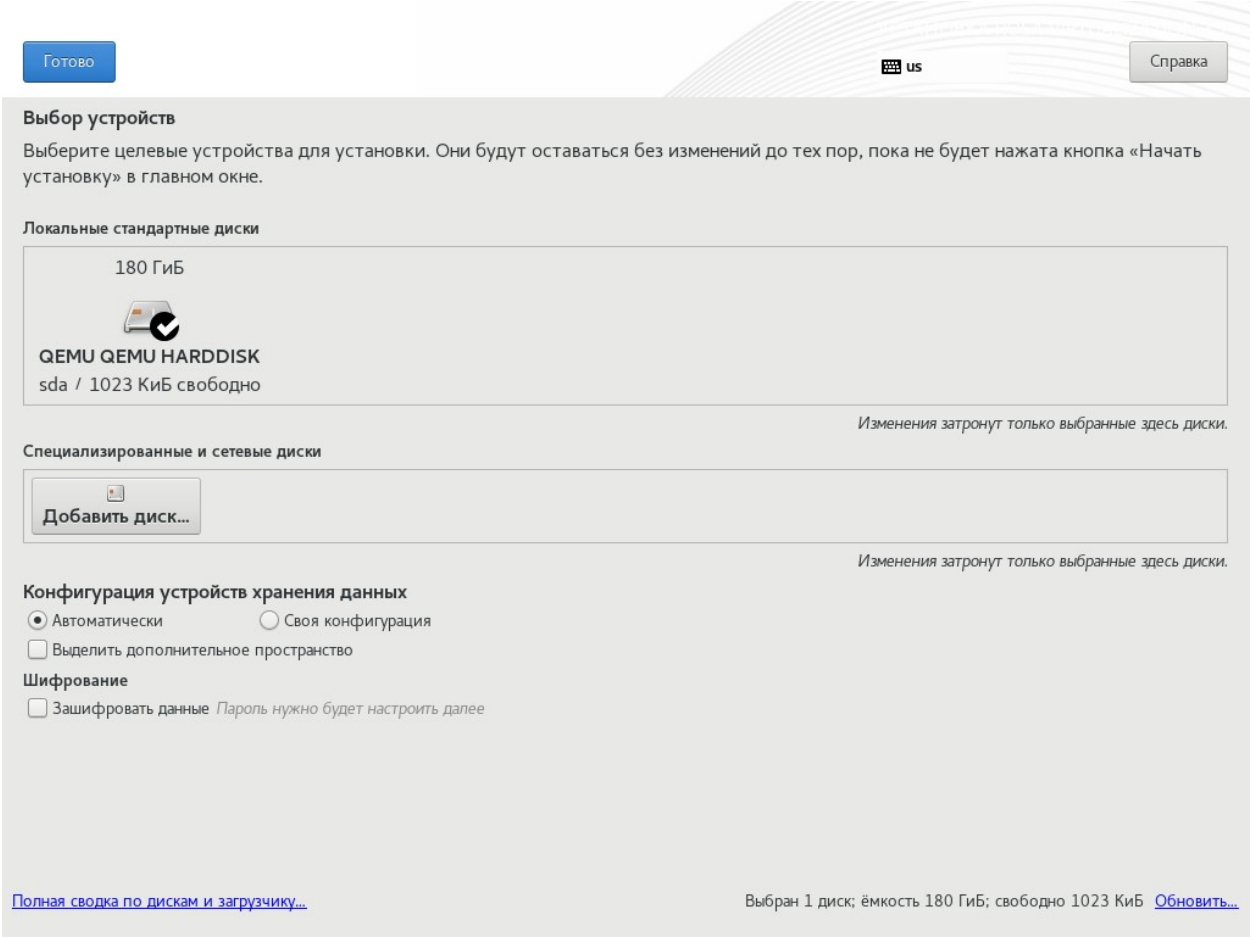

Рисунок 7 – Выбор диска и способа конфигурации разделов

По умолчанию интерфейс отображает только локальные диски, доступные для установки гипервизора. Для каждого диска показаны размер, метка, доступное пространство. Для выбора диска нажмите на блок с информацией о диске. Выбранный для установки диск будет отмечен флажком. При необходимости и наличии выберите несколько дисков для установки. Если диск не выбран, он не будет использоваться при установке.

Примечание – При необходимости добавления дополнительных устройств хранения данных (специализированных накопителей iSCSI, сетевых дисков FCoE SAN, устройств с модулями постоянной памяти NVDIMM) нажмите кнопку Добавить диск.

Для новой установки гипервизора с удалением всех существующих данных с выбранного диска установите переключатель "Конфигурация устройств

хранения данных" в положение "Автоматически". Если на выбранном диске недостаточно свободного места для автоматического разбиения или был установлен флажок "Выделить дополнительное пространство", освободите пространство на диске вручную (см. пункт 3.2.4.6.1).

Для настройки пользовательской конфигурации и создания разделов диска вручную установите переключатель "Конфигурация устройств хранения данных" в положение "Своя конфигурация" (см. пункт 3.2.4.6.2).

Примечание – При необходимости в шифровании разделов диска (кроме /boot) установите флажок "Зашифровать данные" (см. пункт 3.2.4.6.3).

При наличии двух и более дисков, выбранных для установки гипервизора, перейдите по ссылке "Полная сводка по дискам и загрузчику" в интерфейс выбора диска, на котором будет установлен загрузчик (см. пункт 3.2.4.6.4).

Для продолжения настройки конфигурации диска или возвращения в меню "Сводка установки" нажмите кнопку Готово.

3.2.4.6.1. Освобождение дополнительного пространства на диске

Интерфейс освобождения дискового пространства содержит список разделов диска (файловых систем) и элементы управления, позволяющие удалять или уменьшать разделы (рисунок 8).

Важно – При освобождении пространства будут удалены все данные, которые содержит раздел диска (за исключением случаев сжатия раздела), поэтому предварительно рекомендуется создать резервные копии необходимых данных.

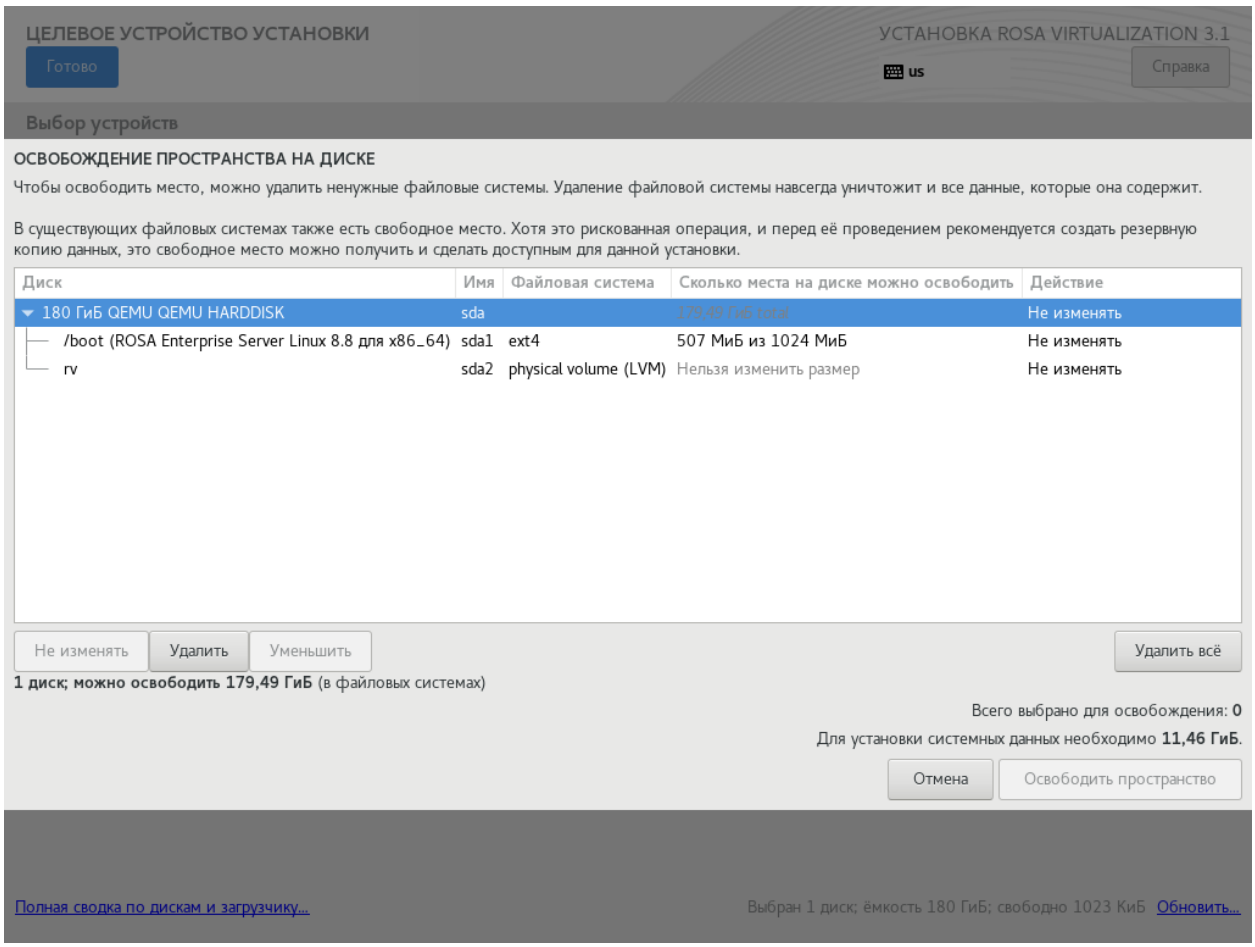

Рисунок 8 – Интерфейс формы для освобождения дискового пространства

В столбце "Сколько места на диске можно освободить" показан потенциально доступный размер дискового пространства.

В столбце "Действие" показан метод освобождения пространства, а сами методы освобождения пространства доступны по нажатию следующих соответствующих кнопок:

– `Не изменять` – не освобождать место в выбранной файловой системе. Это действие установлено по умолчанию;

– `Удалить` – освободить все занятое пространство;

– `Уменьшить` – освободить незанятое пространство в файловой системе. Размер корректируется с помощью ползунка. Это действие недоступно для LVM и RAID;

– `Удалить все` / `Оставить все` – функционирует как переключатель: если выбрать один вариант, название кнопки изменится на второй, и наоборот. Действие применимо ко всем файловым системам.

Выберите файловую систему (раздел) или весь диск, после чего примените необходимые методы освобождения пространства. Когда будет достигнут достаточный объем свободного дискового пространства для продолжения установки (объем зависит от выбранного базового и дополнительного ПО), нажмите кнопку Освободить пространство, которая станет доступной для использования (Рисунок 9).

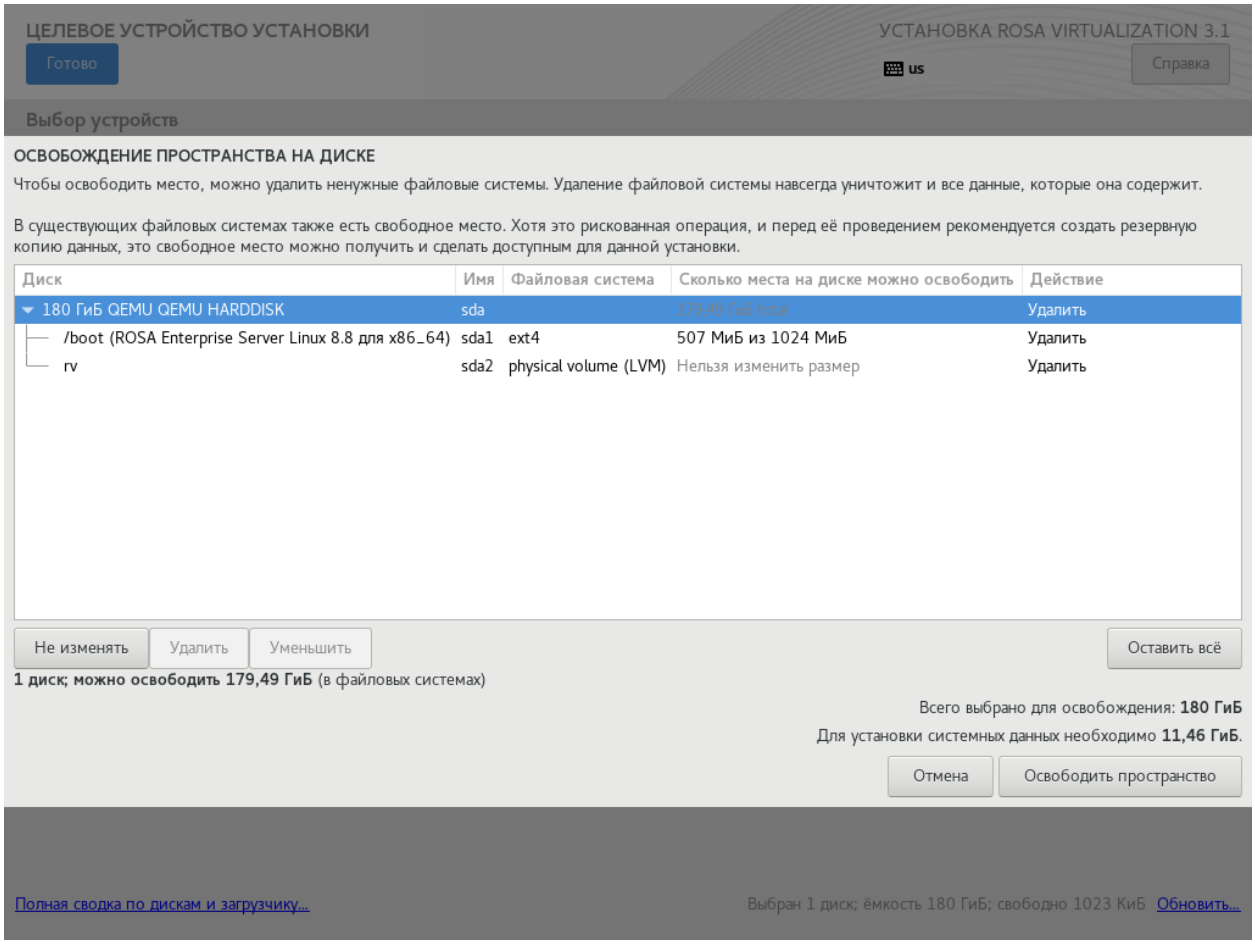

Рисунок 9 – Выбрано для освобождения 180ГБ дискового пространства

3.2.4.6.2 Настройка пользовательской конфигурации разделов диска

Для установки гипервизора рекомендуется создать следующие разделы: /, /boot, /home, /var, /tmp, swap. Раздел подкачки swap не является обязательным, но при ограниченном количестве оперативной памяти его использование настоятельно рекомендуется. Дополнительно администратор установки может создать другие разделы по своему усмотрению.

Для создания раздела диска необходимо создать точку монтирования (автоматически или вручную) и настроить параметры раздела (тип устройства, тип файловой системы раздела).

Если переключатель "Конфигурация устройств хранения данных" был установлен в положение "Своя конфигурация", на экране появится интерфейс создания разделов диска.

3.2.4.6.2.1 Создание схемы разделов LVM с тонким резервированием

Для создания схемы разделов LVM с тонким резервированием выберите в списке пункт "LVM с тонким резервированием" (рисунок 10).

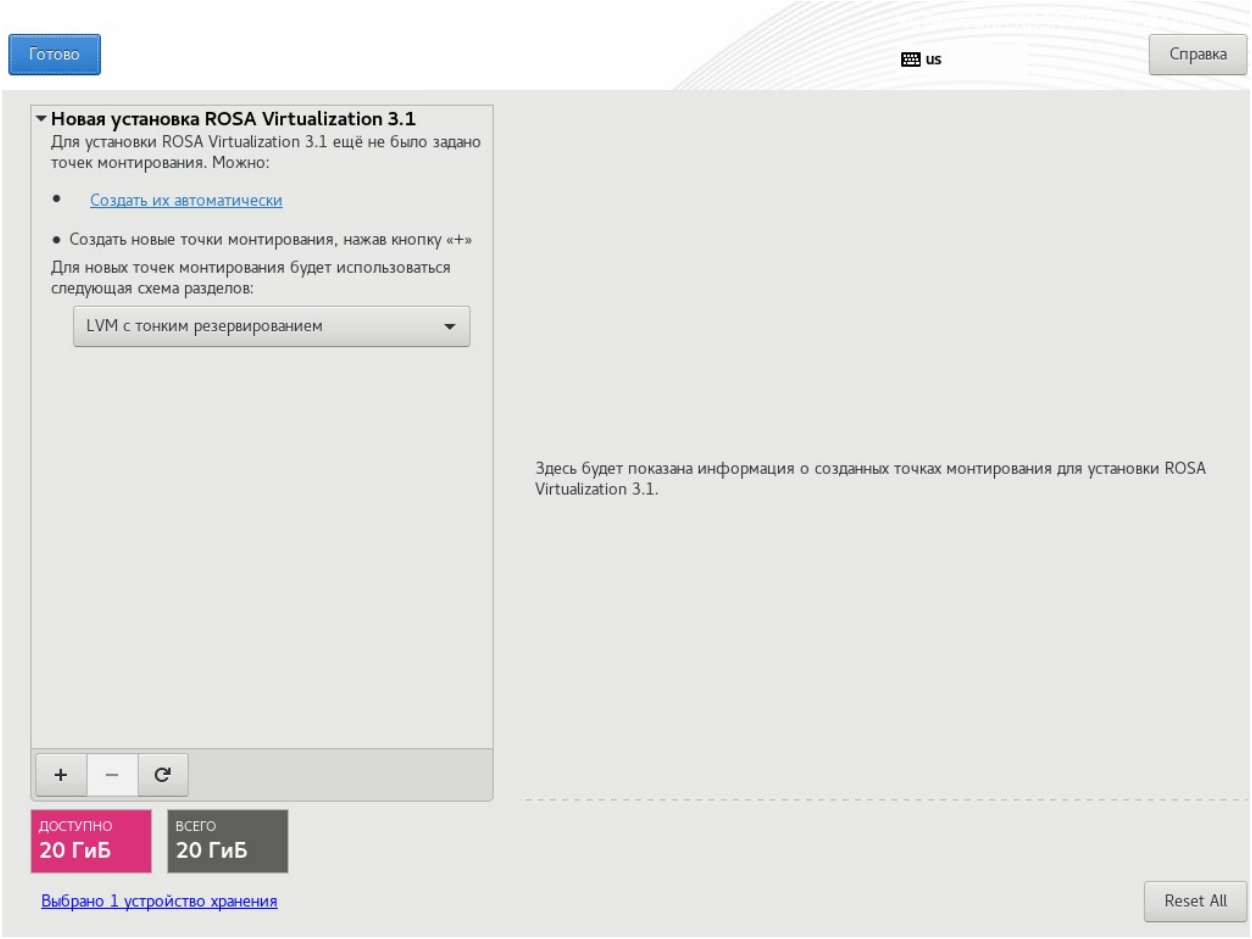

Рисунок 10 – Создание схемы разделов LVM с тонким резервированием

3.2.4.6.2.2 Создание стандартных разделов

Для создания схемы со стандартными разделами выберите в списке пункт "Стандартный раздел" (рисунок 11).

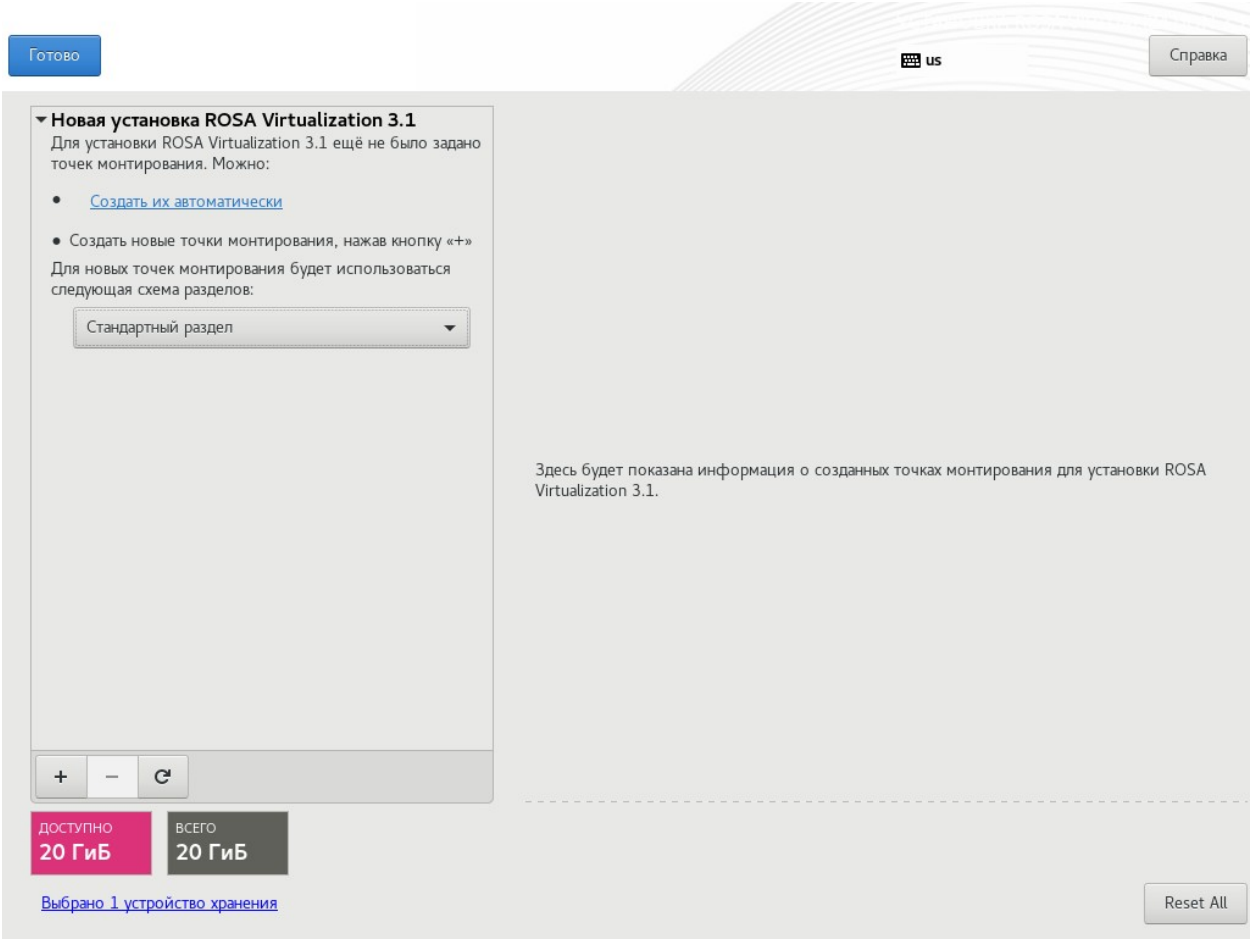

Рисунок 11 – Создание схемы со стандартными разделами

Примечание – При наличии существующих разделов убедитесь, что на диске достаточно места для установки гипервизора (значение свободного дискового пространства приведено в нижней части окна интерфейса). При необходимости в освобождении дискового пространства удалите ненужные разделы. Для удаления выбранного раздела нажмите кнопку –.

3.2.4.6.2.3 Автоматическое создание разделов и точки монтирования

Для того чтобы программа установки автоматически создала разделы и точки монтирования, выберите схему разбиения разделов – "Стандартный раздел", "LVM с тонким резервированием" (схема по умолчанию), "LVM" из выпадающего списка и нажмите ссылку "Создать их автоматически".

В результате будут созданы разделы /, /boot, /home, /var, /tmp и раздел подкачки swap. При этом раздел /boot будет создан как стандартный раздел независимо от ранее выбранного значения схемы разделов.

3.2.4.6.2.4 Создание точки монтирования вручную

Для создания точки монтирования вручную нажмите кнопку +. На экране появится модальное окно "Добавить новую точку монтирования" (рисунок 12).

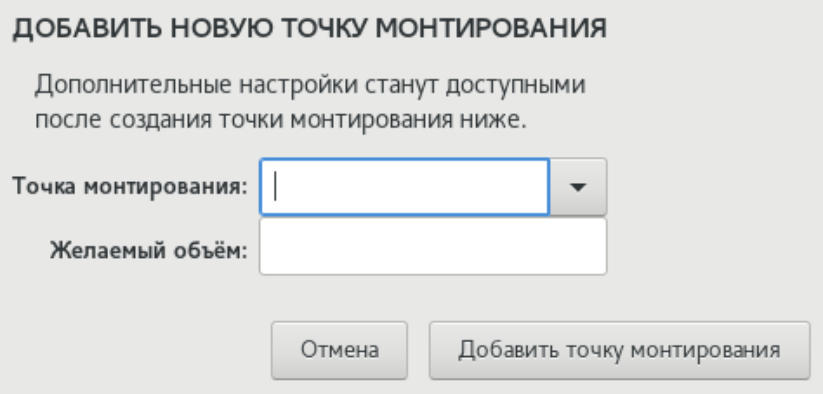

Рисунок 12 – Создание точки монтирования

Выберите раздел для подключения точки монтирования из выпадающего списка в поле "Точка монтирования" (рисунок 12) или введите путь к необходимому разделу вручную. Например, / – для корневого раздела, /boot – для загрузочного раздела.

Укажите размер раздела в мегабайтах, гигабайтах или терабайтах в поле "Желаемый объём", например, 20 ГБ. Если размер не задан или превышает допустимый, будет занято все доступное дисковое пространство.

Нажмите кнопку Добавить точку монтирования (рисунок 12).

После создания точки монтирования станут доступными (в правой области интерфейса) настройки параметров раздела (рисунок 13).

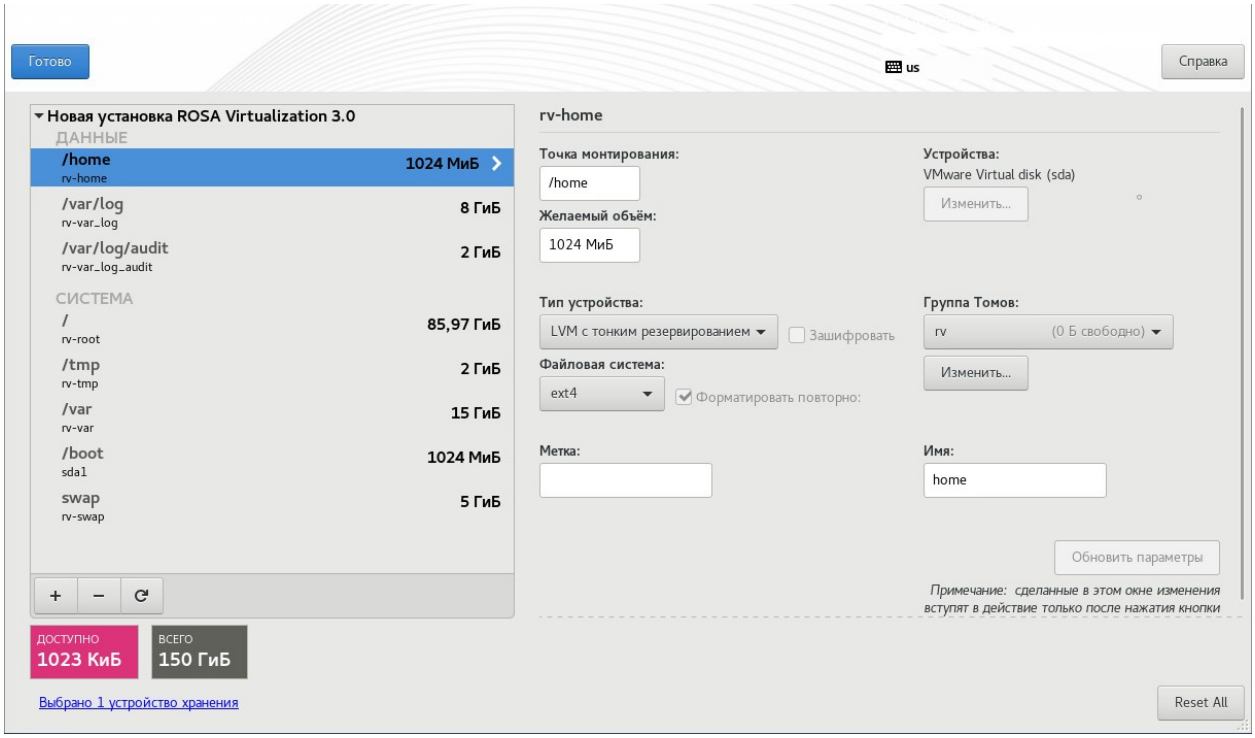

Рисунок 13 – Настройки параметров раздела

Для выбранного раздела доступны следующие параметры настройки:

– Точка монтирования – точка подключения раздела. Например, для корневого раздела введите "/", для загрузочного раздела введите "/boot", для раздела подкачки указывать точку не нужно, достаточно лишь ввести тип "swap";

– Желаемый объём – размер раздела в килобайтах, мегабайтах, гигабайтах или терабайтах. Если единицы не указаны, будут использоваться килобайты;

– Тип устройства – тип раздела. Параметр может принимать следующие значения: "Стандартный раздел", "LVM", "LVM с тонким резервированием" (см. пункт 3.2.4.6.2.6). При наличии двух и более дисков, выбранных для установки гипервизора, также будет доступно значение "RAID";

– Файловая система – тип файловой системы. Параметр может принимать следующие значения: "XFS", "ext4", "ext3", "ext2", "VFAT", "swap", "biosboot" (см. пункт 3.2.4.6.2.9). Справа от поля расположен флажок для форматирования;

– Метка – уникальная метка раздела;

– Имя – имя тома LVM. Имена стандартных разделов присваиваются автоматически и не меняются. Например, разделу /home может быть присвоено имя "sda1".

При необходимости внесите изменения в значения параметров.

Для сохранения изменений нажмите кнопку Обновить параметры. При этом изменения вступят в силу только после начала установки.

Для завершения настройки нажмите кнопку Готово.

На экране появится модальное окно "Сводка изменений" (рисунок 14), где будут перечислены выбранные операции по настройке разделов и файловых систем, включающие создание, изменение размера и удаление.

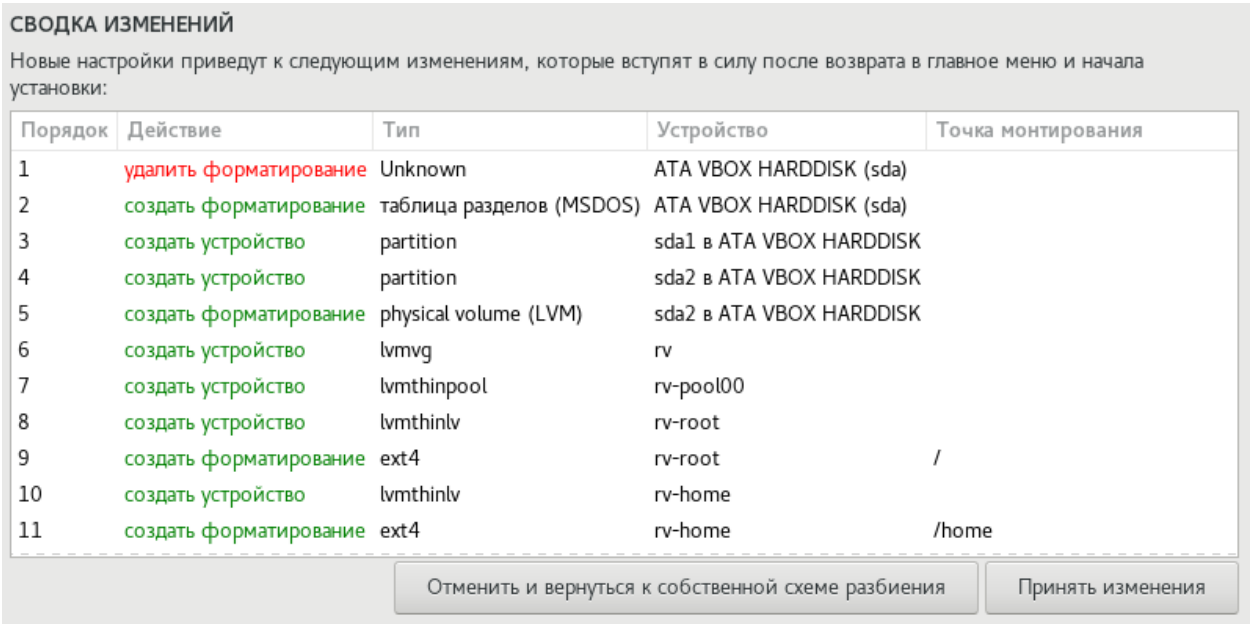

Рисунок 14 – Сводка изменений

Нажмите кнопку Принять изменения.

Для отмены изменений нажмите кнопку Отменить и вернуться к собственной схеме разбиения.

Для того чтобы настроить разделы вручную на другом диске, выберите необходимый диск в окне интерфейса секции "Целевое устройство установки" и установите переключатель "Конфигурация устройств хранения данных" в положение "Своя конфигурация".

3.2.4.6.2.5 Общая схема разбиения диска на разделы

В общем случае при настройке пользовательской конфигурации диска рекомендуется создать следующие разделы:

– корневой раздел файловой системы / (рекомендуемый размер – не менее 10 ГБ);

– загрузочный раздел /boot (рекомендуемый размер – не менее 1 ГБ);

– раздел домашнего каталога /home (рекомендуемый размер – не менее 1 ГБ);

– раздел каталога приложений /var (рекомендуемый размер – не менее 25 ГБ);

– раздел каталога временных файлов /tmp (рекомендуемый размер – не менее 2 ГБ);

– раздел подкачки swap (рекомендуемый размер – не менее 3 ГБ).

Примечания

1) В системах с BIOS, использующих таблицу GPT, необходимо создать стандартный раздел biosboot размером 1 МБ, в то время как при наличии на диске области MBR в этом нет необходимости.

2) В системах с UEFI необходимо создать стандартный раздел /boot/efi размером не менее 50 МБ (рекомендуемый размер – 200 МБ).

3) Некоторые BIOS не поддерживают загрузку с RAID-контроллеров. В таких случаях раздел /boot следует создать на отдельном диске за пределами RAID-массива.

3.2.4.6.2.6 Типы разделов диска

При настройке пользовательской конфигурации диска поддерживается создание разделов следующих типов:

– Стандартный раздел – раздел может содержать файловую систему или пространство подкачки, а также выступать в качестве основы для программного RAID-массива или физического тома LVM;

– LVM – раздел оптимизирует работу жестких дисков. При создании раздела логический том LVM будет создан автоматически;

– LVM с тонким резервированием – раздел перераспределяет свободное пространство между устройствами в зависимости от требований приложений. По мере необходимости пул пространства может наращиваться динамически (см. пункт 3.2.4.6.2.7);

– RAID – каждому диску выделяется один RAID-раздел. При наличии двух и более дисков, выбранных для установки гипервизора, появится возможность создать программный RAID-массив (см. пункт 3.2.4.6.2.8).

3.2.4.6.2.7 Создание группы томов LVM

LVM распределяет пространство между динамически изменяемыми томами. Разделы физического диска представлены в качестве физических томов, которые могут быть объединены в группы. В свою очередь, группы томов могут подразделяться на логические тома, которые по принципу работы аналогичны стандартным дисковым разделам. Таким образом, логические тома LVM функционируют как разделы, которые могут располагаться на нескольких физических дисках.

Группа томов LVM создается через интерфейс настройки параметров раздела. Из выпадающего списка "Тип устройства" выберите значение "LVM с тонким резервированием". В результате появится список "Группа Томов" с именем созданной группы томов LVM.

Для настройки созданной группы томов LVM нажмите кнопку Изменить. На экране появится модальное окно "Настройка группы томов" (рисунок 15).

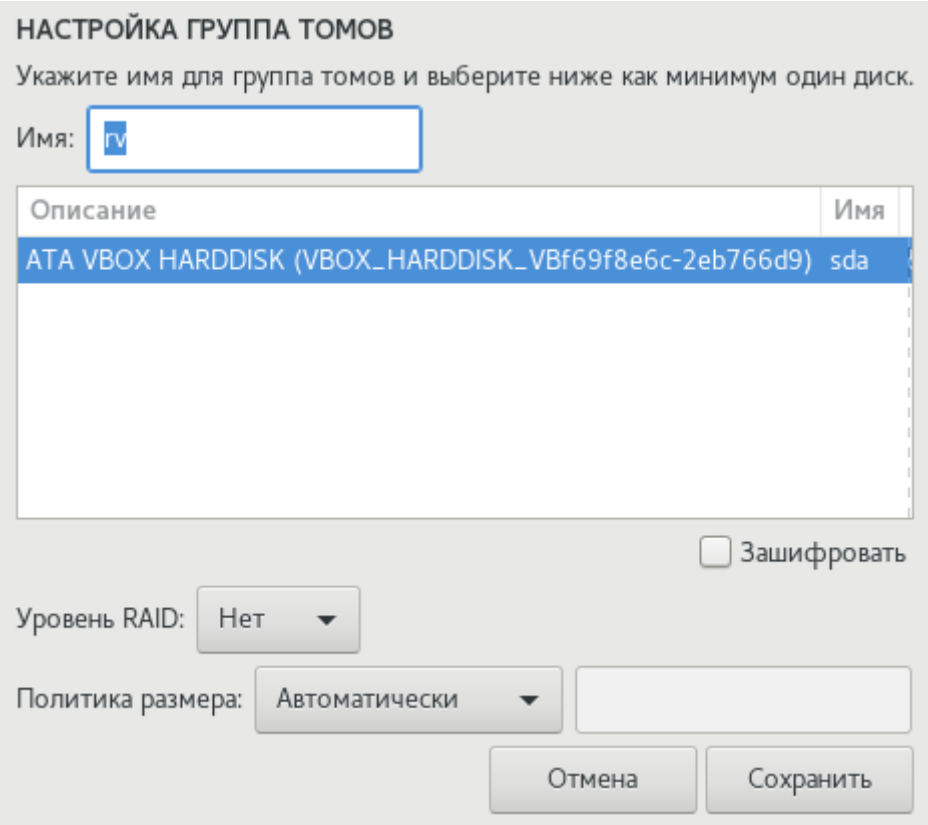

Рисунок 15 – Настройка группы томов LVM

Введите имя для группы томов LVM и выберите диск/диски для размещения раздела.

При необходимости создайте программный RAID-массив для группы томов LVM (см. пункт 3.2.4.6.2.8). Из выпадающего списка "Уровень RAID" выберите одно из следующих значений:

- RAID-0 (производительность);
- RAID-1 (избыточность);
- RAID-4 (проверка ошибок);
- RAID-5 (распределенная проверка ошибок);
- RAID-6 (проверка ошибок с избыточностью);
- RAID-10 (производительность, избыточность).

Примечание – Для шифрования раздела группы томов LVM установите флажок "Зашифровать".

Определите размер группы томов LVM. Из выпадающего списка "Политика размера" выберите одно из следующих значений:

– Автоматически – размер группы томов будет определен с учетом заданных параметров. Вариант является оптимальным, если не требуется оставлять свободное пространство в пределах группы томов;

– Как можно больше – выделяется максимально возможный размер независимо от конфигурации. Вариант подходит для хранения данных в LVM с возможной перспективой добавления новых или наращивания существующих томов;

– Фиксированный – точный размер группы томов устанавливается вручную. Введите в поле необходимое значение размера группы томов.

Нажмите кнопку Сохранить.

Если для создания RAID-массива не хватает дисков, в нижней части окна появится сообщение с рекомендуемым количеством.

Примечание – Загрузочный раздел /boot не может располагаться в пределах логического тома LVM.

3.2.4.6.2.8 Создание программного RAID-массива

RAID-массивы объединяют несколько устройств хранения для обеспечения должного уровня производительности и отказоустойчивости.

RAID-массив создается один раз, после чего состав RAID-массива можно корректировать посредством добавления или исключения дисков.

На каждом диске может быть создан один RAID-раздел. Таким образом, максимальный уровень RAID определяется количеством дисков.

При наличии двух и более дисков, выбранных для установки гипервизора, появится возможность создать программный RAID-массив через интерфейс настройки параметров раздела. Из выпадающего списка "Тип устройства" выберите значение "RAID". В результате появится список "Уровень RAID" для выбора одного из следующих значений:

– RAID-0 (производительность) – данные распределяются между несколькими дисками. RAID-0 обеспечивает высокий уровень производительности за счет объединения дисков в одно виртуальное устройство. Надежность RAID-0 невысокая, так как отказ одного диска приведет к сбою всего массива. Для создания RAID-0 необходимо как минимум два раздела RAID;

– RAID-1 (избыточность) – использует зеркалирование за счет копирования данных на все диски в составе массива. Дополнительные устройства повышают уровень избыточности. Для создания RAID-1 необходимо как минимум два раздела RAID;

– RAID-4 (проверка ошибок) – данные распределяются между несколькими дисками, но при этом один диск служит для хранения информации о четности, что помогает восстановить данные в случае сбоя. Недостаток такой организации заключается в том, что информация о четности хранится на одном диске, что представляет риск для общей производительности массива. Для создания RAID-4 необходимо как минимум три раздела RAID;

– RAID-5 (распределенная проверка ошибок) – контрольные суммы и данные циклически распределяются между элементами массива. RAID-5 более востребован по сравнению с RAID-4 благодаря параллельной обработке данных. Для создания RAID-5 необходимо как минимум три раздела RAID;

– RAID-6 (проверка ошибок с избыточностью) – аналогичен RAID-5, но контрольные данные копируются на два устройства. Для создания RAID-6 необходимо как минимум четыре раздела RAID (два раздела для основных данных и два раздела для контрольных данных);

– RAID-10 (производительность, избыточность) – данные распределяются между зеркальными наборами дисков. RAID-10 из четырех разделов будет включать две зеркальные пары RAID-1. При этом данные последовательно распределяются между парами аналогично RAID-0. Для создания RAID-10 необходимо как минимум четыре раздела RAID.

Для сохранения изменений нажмите кнопку Обновить параметры.

Если для создания RAID-массива не хватает дисков, в нижней части окна появится сообщение с рекомендуемым количеством.

3.2.4.6.2.9 Типы файловых систем

При настройке пользовательской конфигурации диска поддерживается создание файловых систем следующих типов:

– XFS – высокопроизводительная масштабируемая файловая система, размер которой может достигать 16 эксабайт (16 миллионов терабайт). XFS поддерживает файлы размером до 8 эксабайт (8 миллионов терабайт) и структуры каталогов с десятками миллионов записей и включает функции журналирования метаданных, что гарантирует быстрое восстановление в случае сбоя, а также поддерживает дефрагментацию и изменение размера без необходимости отключения файловой системы. Максимально допустимый объем файловой системы XFS составляет 500 ТБ;

– ext4 – файловая система, созданная на основе ext3. Преимуществами ext4 являются поддержка больших файловых систем и файлов, быстрое и

эффективное распределение пространства, отсутствие ограничений на число подкаталогов в одном каталоге, быстрая проверка файловой системы и надежное ведение журналов. Максимально допустимый объем файловой системы ext4 составляет 50 ТБ;

– ext3 – файловая система, созданная на основе ext2. Главным преимуществом ext3 является поддержка журналов, что сокращает время восстановления файловой системы благодаря отсутствию необходимости в проверке с использованием утилиты fsck;

– ext2 – файловая система поддерживает стандартные типы файлов Unix (обычные файлы, каталоги, символьные ссылки) и позволяет присваивать им имена длиной до 255 знаков;

– VFAT – файловая система Linux, совместимая с FAT и поддерживающая длинные имена файлов ОС семейства Windows;

– swap – раздел подкачки для организации виртуальной памяти. Если в ОЗУ не хватает места для обработки данных, неактивные фрагменты перемещаются в область подкачки, освобождая место для новых страниц;

– biosboot – небольшой стандартный раздел для загрузки систем на базе BIOS с дисков с таблицей разделов GPT.

Примечание – При работе с файлами большого размера (например, диски виртуальных машин) рекомендуется использовать файловую систему XFS.

3.2.4.6.3 Шифрование разделов диска

Шифрование разделов диска позволяет защитить конфиденциальные данные от неавторизованного доступа к серверному оборудованию, но накладывает дополнительные эксплуатационные ограничения.

Для шифрования разделов диска используется механизм LUKS.

Если в секции параметров "Целевое устройство установки" был установлен флажок "Зашифровать данные", на экране появится интерфейс создания пароля доступа к зашифрованным данным (рисунок 16).

Примечание – Пароль доступа надо будет вводить каждый раз при загрузке ОС гипервизора, поэтому шифрование разделов диска может быть нецелесообразным в промышленном режиме функционирования ROSA Virtualization, так как снижается общая производительность работы с платформой виртуализации. Также обратите внимание, что в случае утери парольной фразы зашифрованные разделы и их данные будут недоступны – восстановить доступ будет невозможно.

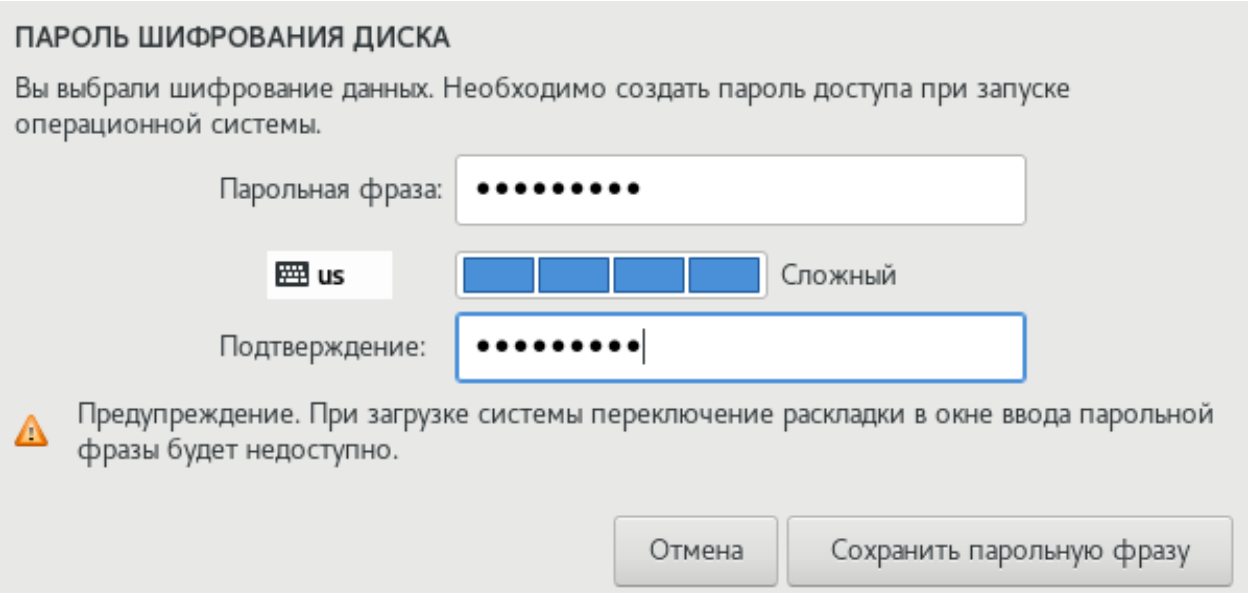

Рисунок 16 – Создание пароля доступа при использовании шифрования диска

В поле "Парольная фраза" введите парольную фразу, при этом обратите внимание на раскладку клавиатуры (рисунок 16). Для изменения раскладки клавиатуры нажмите на значок . Если введенный пароль является слабым, на экране появится информационное сообщение с предупреждением.

В поле "Подтверждение" введите пароль доступа еще раз, после чего нажмите кнопку `Сохранить парольную фразу`.

3.2.4.6.4 Выбор диска для установки загрузчика

Загрузчик – первая программа, запускаемая после включения компьютера, которая передает управление ядру ОС.

ОС гипервизора использует загрузчик GRUB2.

При наличии двух и более дисков, выбранных для установки гипервизора, потребуется вручную определить необходимый загрузочный диск (рисунок 17). Переход по ссылке "Полная сводка по дискам и загрузчику" откроет интерфейс выбора диска, на котором будет установлен загрузчик.

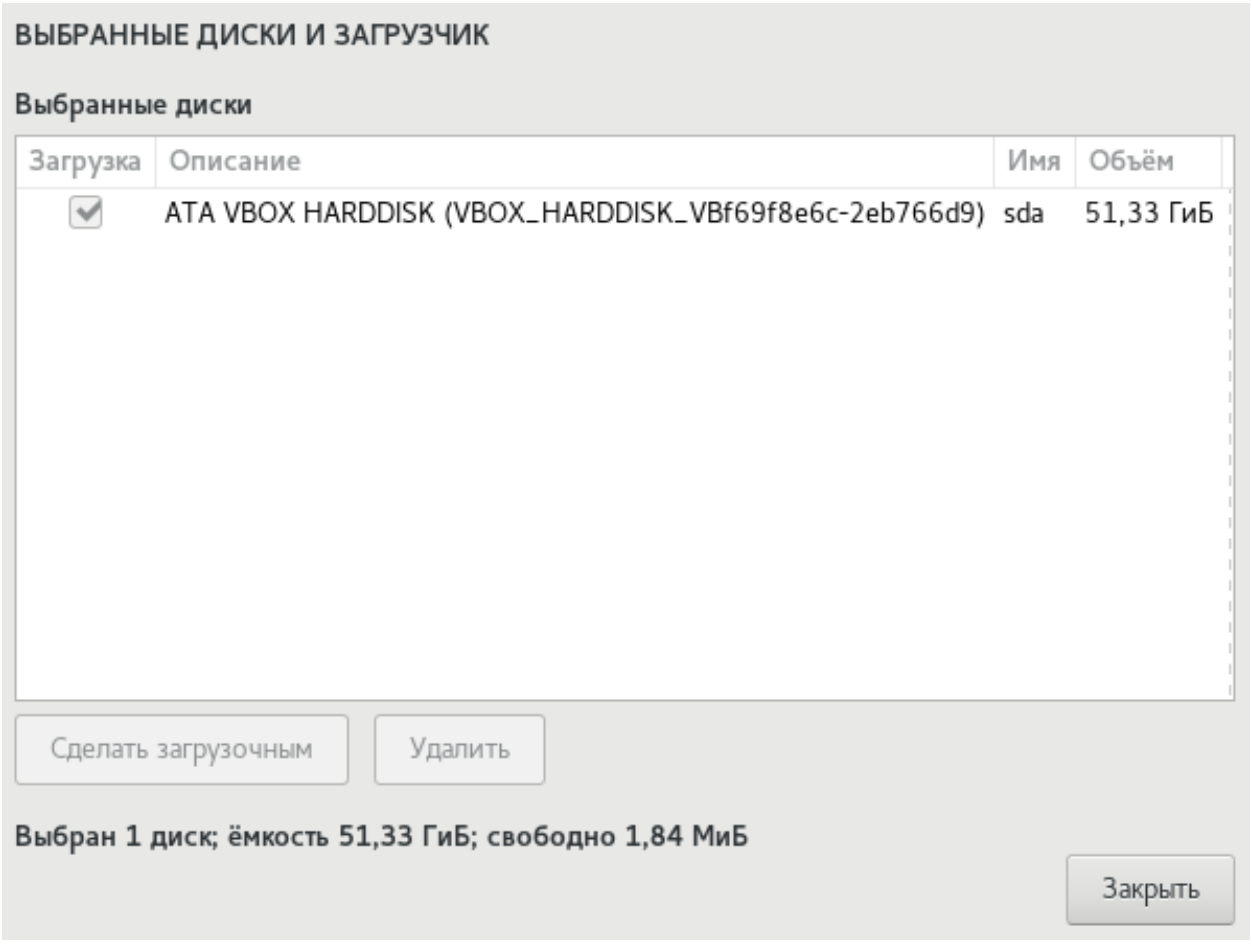

Рисунок 17 – Выбор диска для установки загрузчика

По умолчанию загрузочное устройство отмечено флажком. Чтобы установить загрузчик на другое устройство, выберите его из списка и нажмите на кнопку `Сделать загрузочным`.

Для возвращения к интерфейсу секции "Целевое устройство установки" нажмите кнопку `Закрыть` (рисунок 17).

По умолчанию загрузчик GRUB2 будет установлен в область MBR для диска (с корневой файловой системой) размером меньше 2 ТБ или в область GPT – для диска размером больше 2 ТБ.

3.2.4.7 Имя хоста и сетевые подключения гипервизора

Интерфейс секции "Сеть и имя хоста" предназначен для указания имени хоста и настройки параметров сетевых адаптеров гипервизора (рисунок 18).

Важно – Задание имени хоста является обязательным для проведения успешной установки системы.

Важно – Для установки и начала эксплуатации ROSA Virtualization необходимо настроить как минимум один сетевой адаптер. Подключение остальных сетевых адаптеров допускается выполнить после установки гипервизора с помощью средств администрирования.

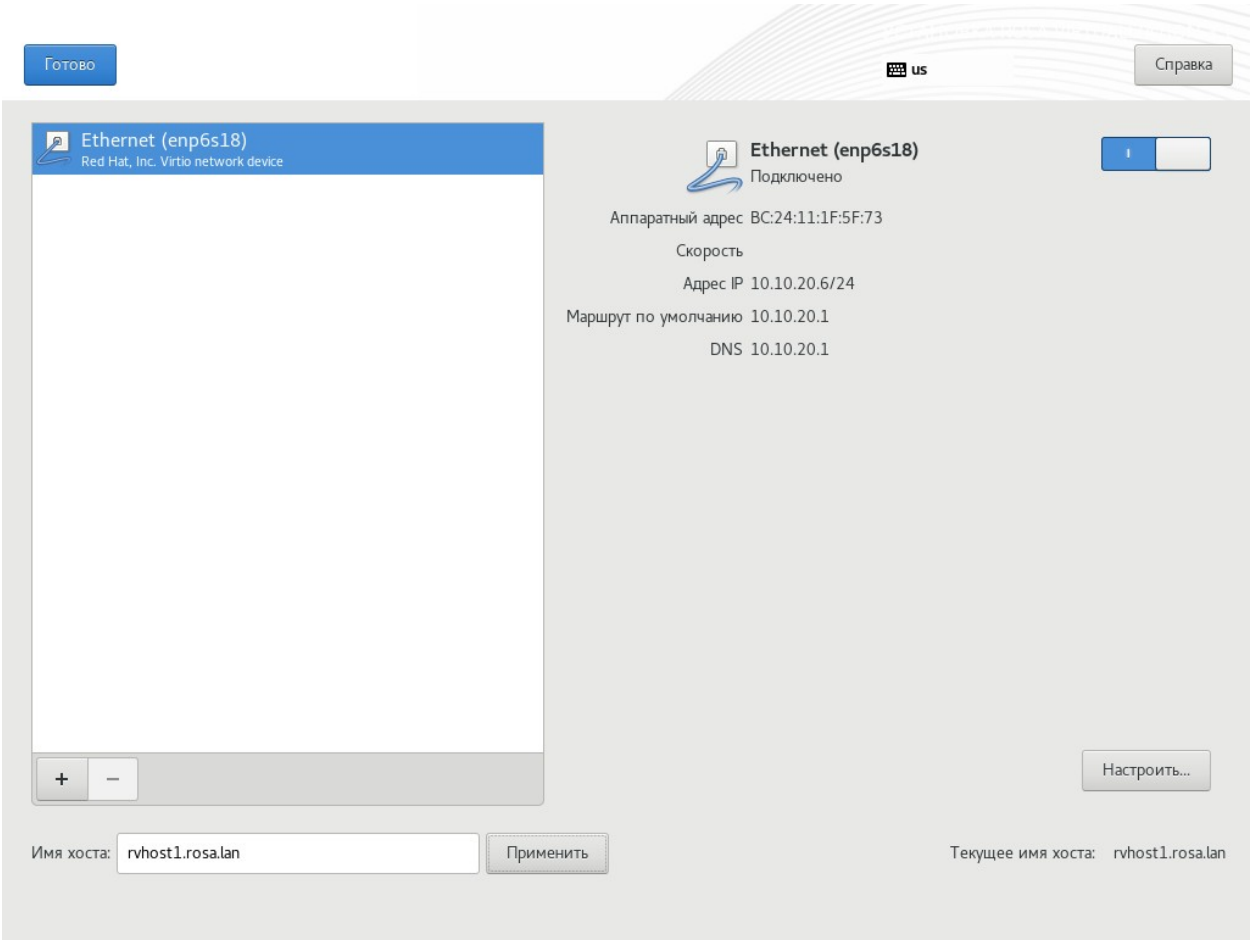

Рисунок 18 – Сетевые адаптеры и имя хоста

3.2.4.7.1 Имя хоста

Имя хоста гипервизора является необходимым параметром для конфигурирования системы на этапе предварительной подготовки к установке

В поле "Имя узла" введите полное доменное имя хоста гипервизора (например, "rvhost1.rosa.lan") и нажмите кнопку Применить. Каждый хост с установленным гипервизором должен иметь уникальное имя в домене.

Важно – Имя хоста гипервизора должно быть действительным именем DNS, в котором разрешается использовать только цифры, символы алфавита и дефис ("-"). Другие символы в имени хоста (например, нижнее подчеркивание) приведут к сбоям в работе службы DNS. Кроме того, имя хоста должно состоять

только из символов в нижнем регистре, прописные буквы в имени хоста не допускаются.

3.2.4.7.2 Сетевые подключения

Программа установки гипервизора автоматически найдет доступные сетевые интерфейсы и отобразит их списком в левой части окна секции "Сеть и имя хоста".

Для подключения сетевого интерфейса выберите необходимый адаптер в списке и установите переключатель в положение "|", а для отключения – в положение "O".

Для настройки параметров выберите необходимый сетевой интерфейс в списке и нажмите кнопку Настроить. На экране появится окно с параметрами интерфейса (перечень доступных параметров зависит от типа сетевого соединения) (рисунок 19).

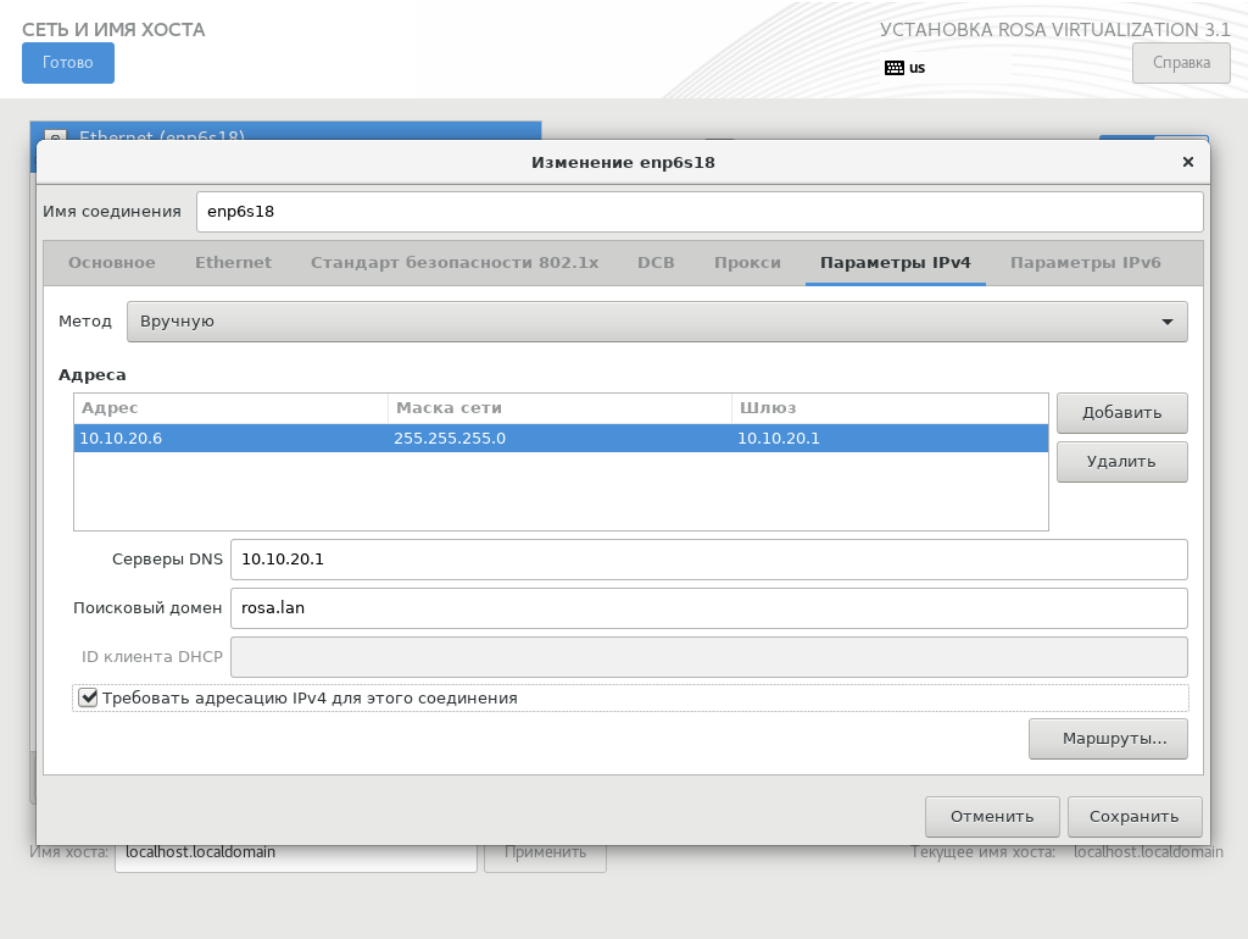

Рисунок 19 – Параметры сетевого соединения: IPv4, подключение вручную, "Требовать адресацию IPv4 для этого соединения"

Для автоматического подключения необходимого сетевого интерфейса в процессе загрузки ОС гипервизора установите флажок "Автоматически подключаться к этой сети, когда она доступна" во вкладке "Основное" с общими параметрами данного интерфейса.

3.2.4.7.2.1 Настройка параметров сетевого подключения с автоматическим конфигурированием по протоколу DHCP

По умолчанию сетевые параметры IPv4 и IPv6 настраиваются автоматически по протоколу DHCP (рисунок 20).

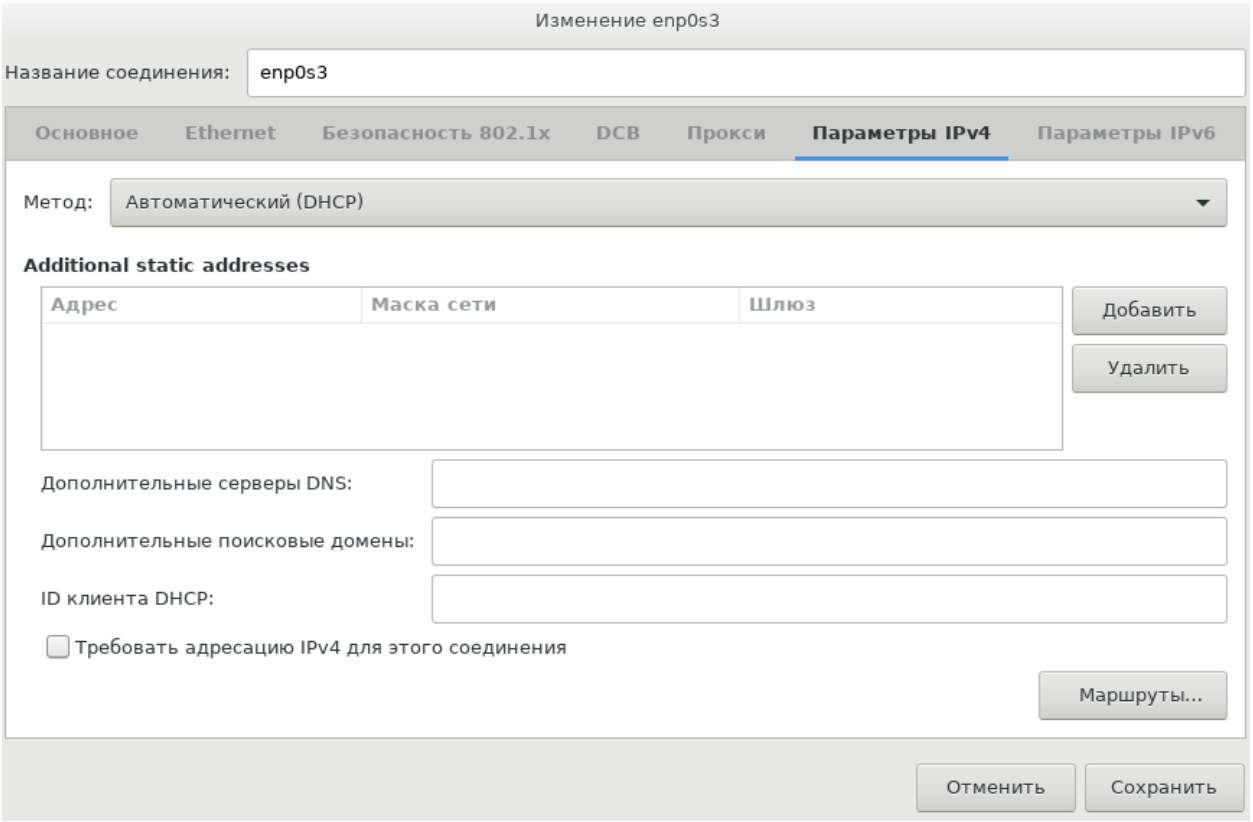

Рисунок 20 – Настройка IPv4 с автоматическим конфигурированием по протоколу DHCP

Примечание – При использовании автоматической настройки сетевых параметров по протоколу DHCP необходимо наличие в сети DHCP сервера и добавление хоста на корпоративный DNS-сервер, который используется для разрешения имен хостов в домене.

3.2.4.7.2.2 Настройка параметров сетевого подключения с использованием статического IP-адреса

Для настройки сетевого соединения с использованием статического IP-адреса перейдите на вкладку "Параметры IPv4" и выберите из выпадающего списка "Метод" значение "Вручную" (рисунок 21).

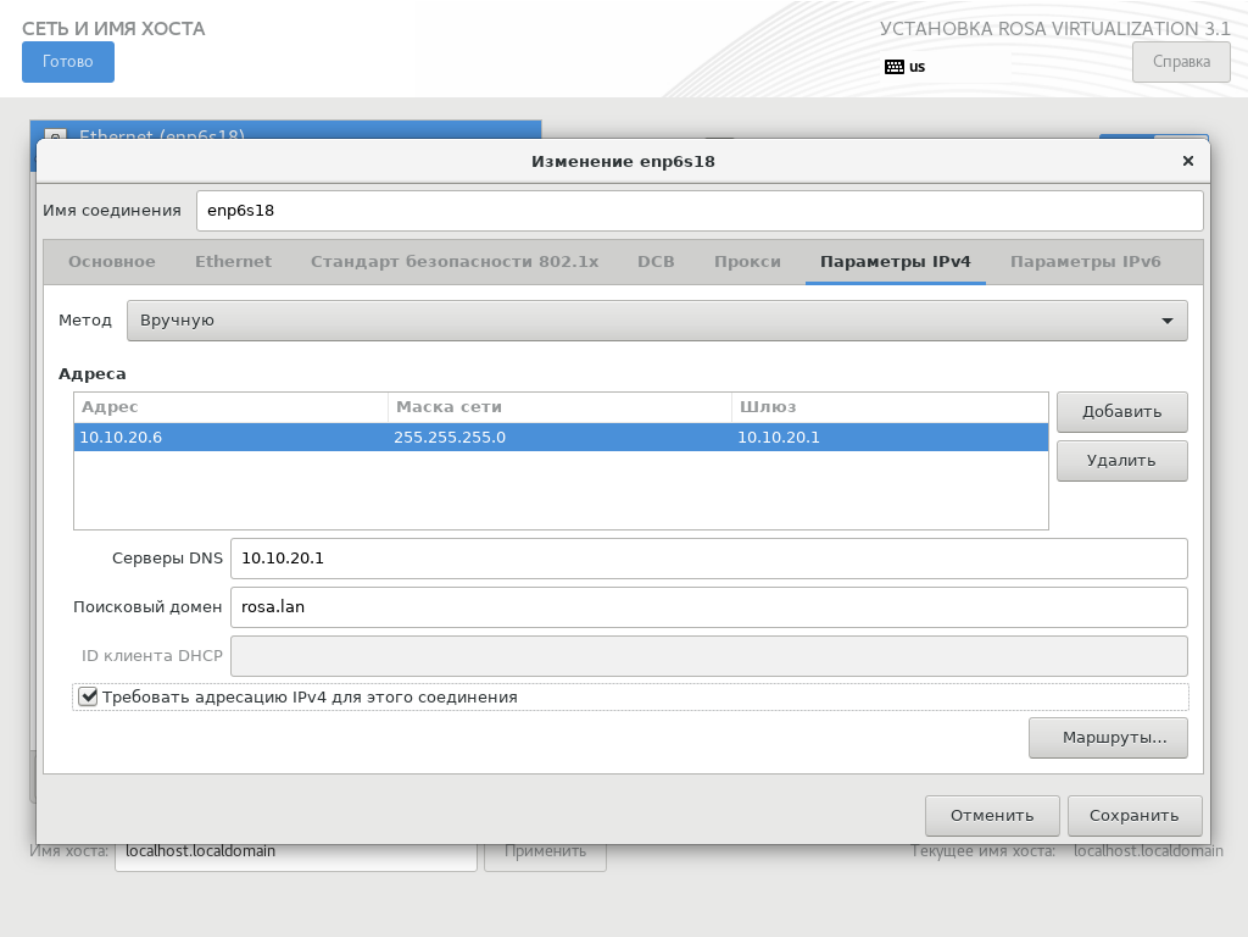

Рисунок 21 – Настройка параметров IPv4: вручную (статический IP-адрес), IP-адрес, маска подсети, шлюз, DNS-сервер, шлюз и поисковый домен

Нажмите кнопку Добавить и введите в соответствующие поля необходимые значения статического IP-адреса интерфейса, маски сети и шлюза.

Важно – Перед присвоением хосту статического IP-адреса убедитесь, что данный IP адрес не используется другими хостами в сети и не входит в диапазон IP-адресов, автоматически выделяемых DHCP сервером.

В поле "Серверы DNS" введите значение IP-адреса корпоративного и/или внешнего публичного DNS-сервера, который используется для разрешения имен хостов в домене (при необходимости укажите несколько IP-адресов DNS-серверов через запятую).

В поле "Поисковый домен" укажите наименование домена (например, "rosa.lan").

Установите флажок "Требовать адресацию IPv4 для этого соединения".

Для применения сделанных изменений нажмите кнопку Сохранить (рисунок 21).

Для добавления и настройки нового виртуального интерфейса (VLAN и интерфейсы, созданные посредством объединения (группировки) физических сетевых адаптеров) нажмите кнопку + в левой нижней части окна секции "Сеть и имя хоста".

Для удаления выбранного сетевого интерфейса из списка программы установки нажмите кнопку –.

После настройки сетевых параметров нажмите кнопку Готово для возвращения в меню "Сводка установки" (рисунок 21).

3.2.4.8 Пароль для учетной записи суперпользователя root

Учетная запись суперпользователя root предназначена для администрирования ROSA Virtualization. Для учетной записи суперпользователя root крайне важно установить надежный пароль, чтобы исключить возможность несанкционированного доступа к ресурсам ROSA Virtualization.

При выборе и использовании пароля рекомендуется следовать следующим правилам:

– длина пароля должна быть не менее 8 символов;
– используйте для пароля не только буквы и цифры, но и спецсимволы ("@", "#", "$", "&", "*", "%", "!" и т.п.);
– используйте для пароля как строчные (в нижнем регистре), так и прописные (в верхнем регистре) буквы;
– не используйте для пароля общеупотребительные слова, в том числе имена собственные. Надежный пароль должен представлять собой бессмысленную комбинацию символов;
– никогда не записывайте пароль (ни на электронных, ни на бумажных носителях);
– никому не сообщайте пароль;
– запомните пароль, чтобы не забыть его.

В окне секции "Пароль root" введите и подтвердите пароль для учетной записи суперпользователя (рисунок 22).

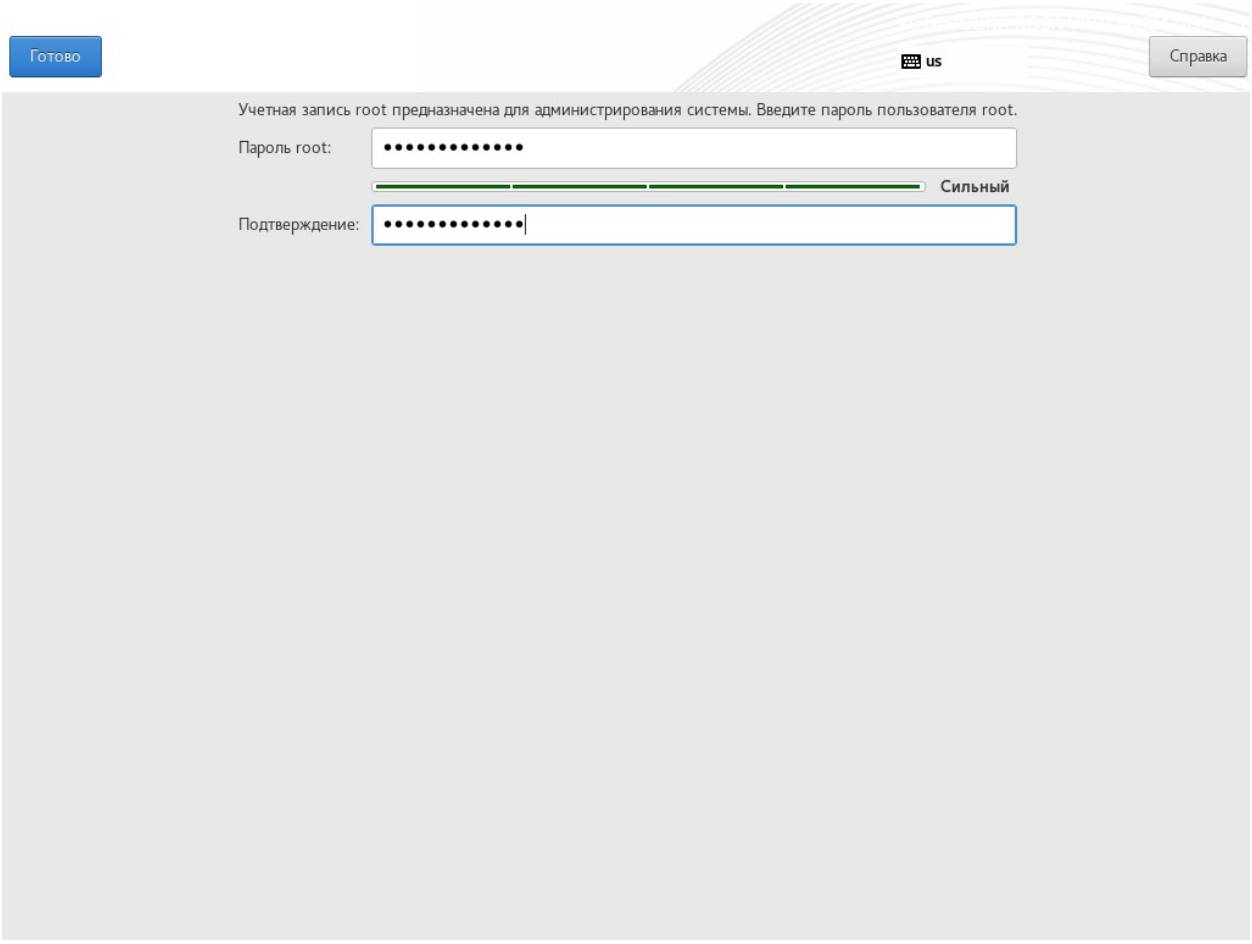

Рисунок 22 – Ввод и подтверждение пароля учетной записи root

Примечание – При вводе слишком простого пароля программа установки выдаст соответствующее предупреждение, и в этом случае рекомендуется сменить пароль на более надежный.

После ввода пароля нажмите кнопку Готово для возвращения в меню "Сводка установки".

3.2.5 Начало и ход процесса установки

Для старта процесса установки гипервизора нажмите кнопку Начать установку, которая станет доступной в меню "Сводка установки" после настройки обязательных параметров (рисунок 23).

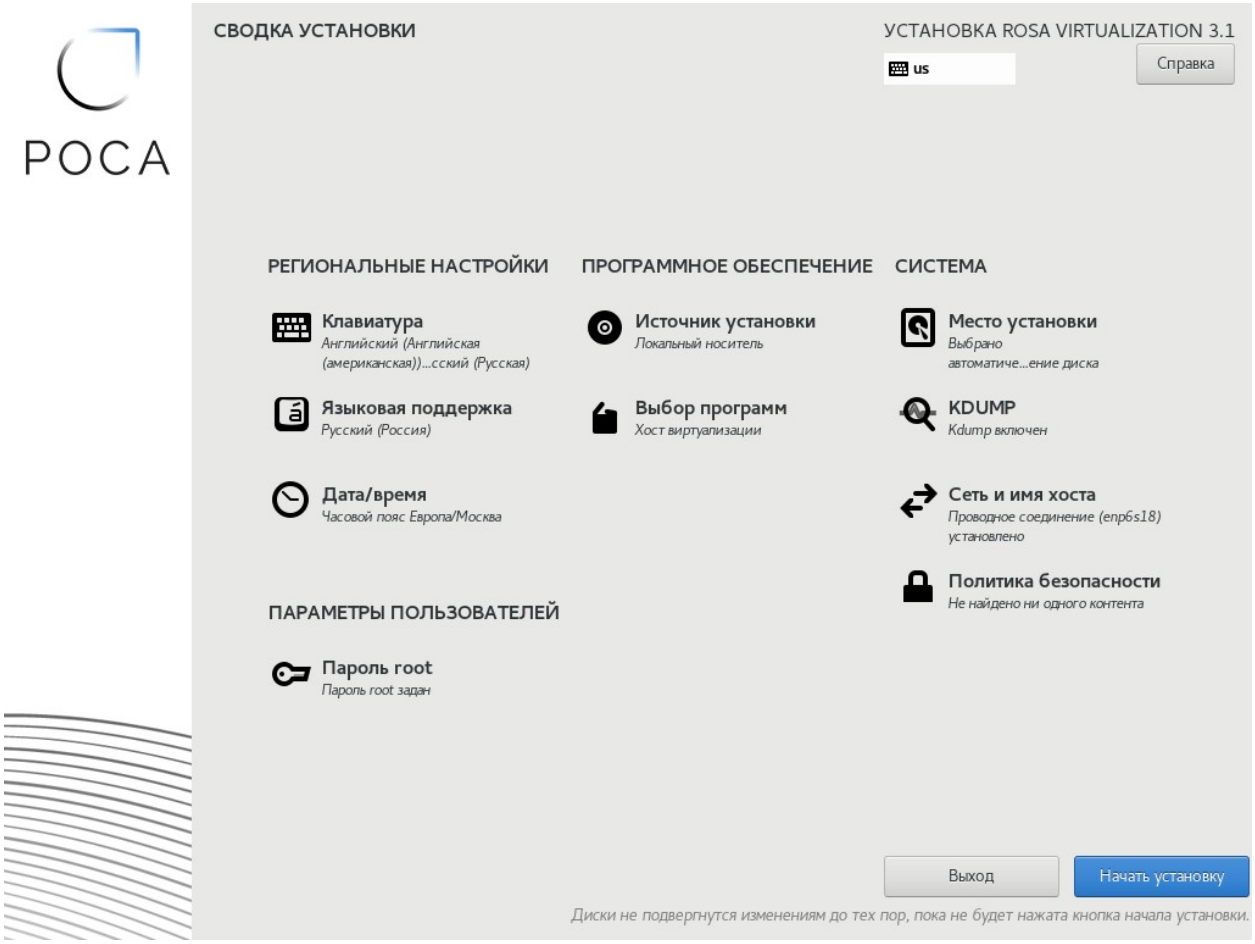

Рисунок 23 – Сводка установки

Программа установки Anaconda выделит место на выбранном диске и начнет установку гипервизора.

Ход процесса установки отображается на экране в виде индикатора прогресса (рисунок 24).

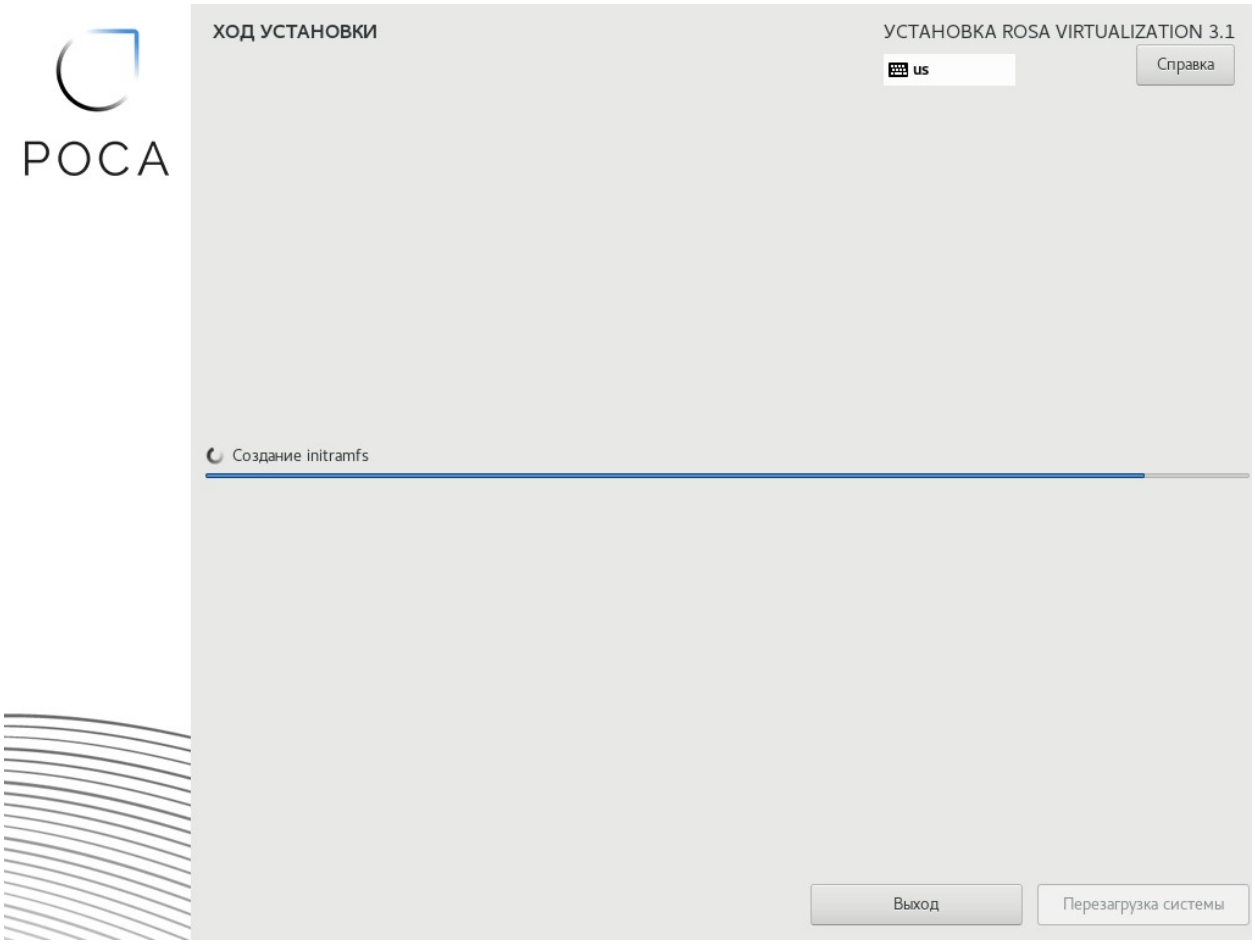

Рисунок 24 – Процесс установки ROSA Virtualization

3.2.6 Завершение установки

Для завершения установки нажмите кнопку `Перезагрузка системы`, которая станет доступной после успешного окончания процесса инсталляции гипервизора (рисунок 25).

Рисунок 25 – Завершение процесса установки

Извлеките DVD- или USB-накопитель, с которого выполнялась установка.

После перезагрузки системы выполните вход в веб-интерфейс администрирования хоста гипервизора для продолжения настройки и установки компонентов ROSA Virtualization.

Примечание – Для развертывания ROSA Virtualization в базовой конфигурации установите как минимум 3 гипервизора на различных хостах.

3.2.7 Вход в веб-интерфейс хоста гипервизора

Для доступа к веб-интерфейсу хоста гипервизора введите в адресной строке браузера (на внешней рабочей станции) доменное имя или IP-адрес хоста гипервизора с обязательным указанием порта подключения – "9090", например:

```
https://rvhost1.rosa.lan:9090
```

На экране появится окно авторизации интерфейса.

Примечание – При первом входе в веб-интерфейс гипервизора в браузере может отобразиться "Предупреждение: Вероятная угроза безопасности". В этом случае нажмите кнопку Дополнительно, а затем на кнопку Принять риск и продолжить. Предупреждение о безопасности связано отсутствием в браузере сертификата, используемого при установке хоста виртуализации "rvhost1".

Для первичной настройки и администрирования хоста гипервизора осуществите вход в интерфейс от имени учетной записи суперпользователя root, используя пароль, выбранный ранее (см. п. 3.2.4.8).

Для входа в интерфейс введите имя (логин) и пароль пользователя в соответствующие поля, после чего нажмите кнопку Вход в систему (рисунок 26).

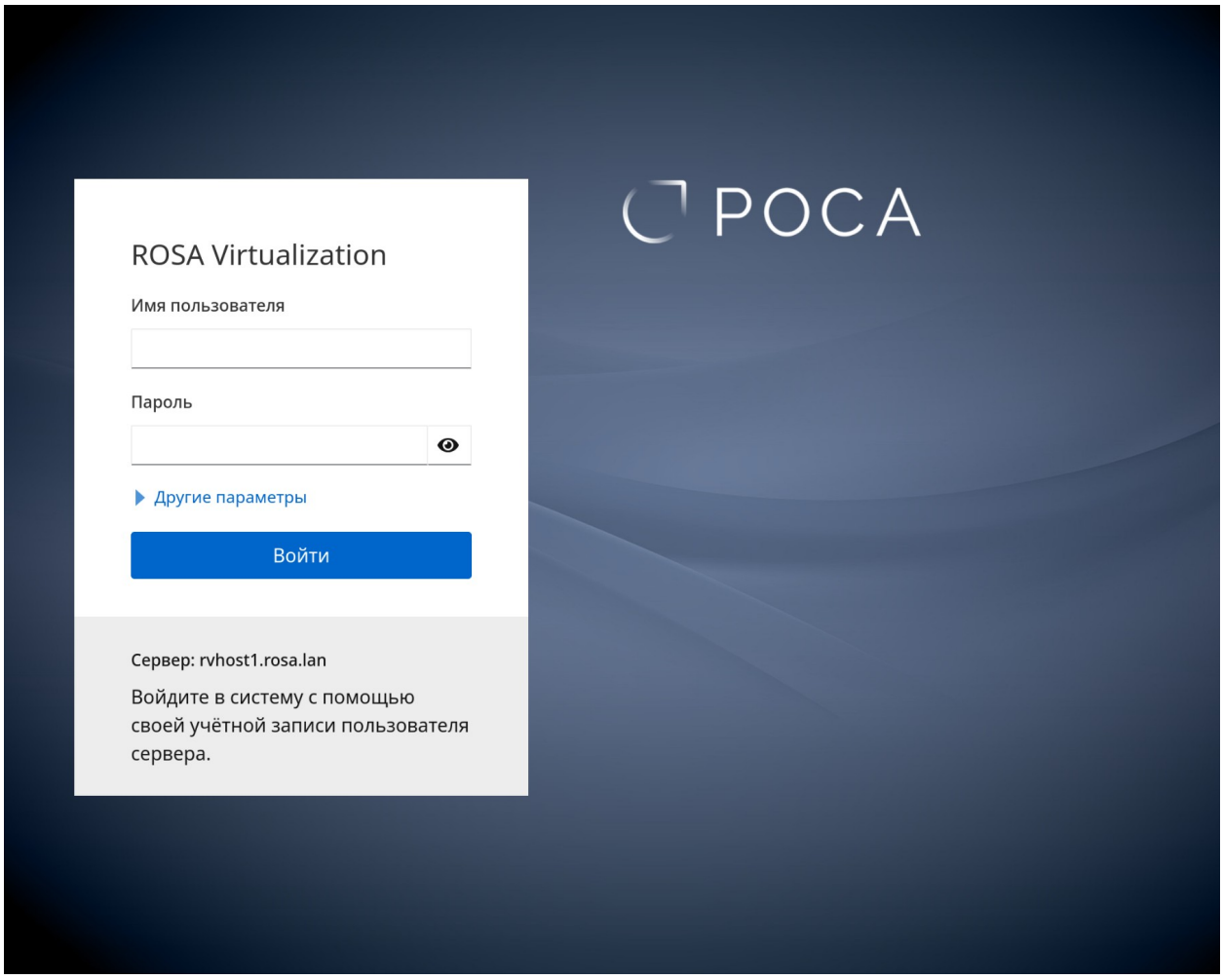

Рисунок 26 – Окно авторизации веб-интерфейса хоста гипервизора

В случае успешной авторизации откроется страница интерфейса (вкладка) "Обзор", которая загружается по умолчанию и содержит общие сведения о хосте гипервизора (рисунок 27).

Для перемещения по страницам интерфейса используйте необходимые вкладки панели навигации.

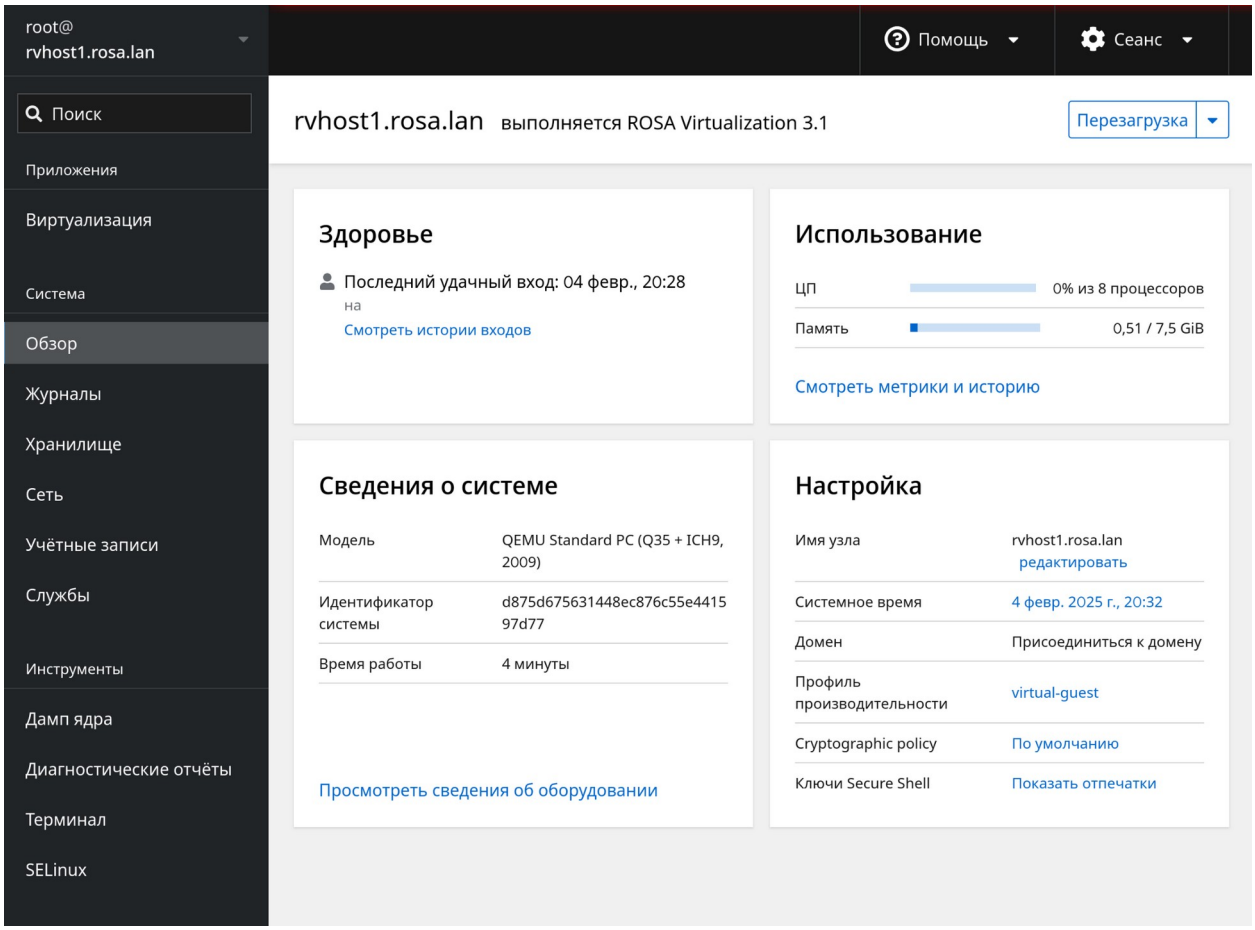

Рисунок 27 – Интерфейс хоста гипервизора (Панель навигации, секции "Здоровье", "Использование", "Сведения о системе", "Настройка")

3.3 Настройка системных параметров хоста гипервизора

Настройка параметров системного окружения осуществляется администратором в консоли каждого из хостов с установленным гипервизором.

3.3.1 Доступ к консоли с использованием веб-интерфейса

Для доступа к консоли в веб-интерфейсе хоста перейдите на вкладку "Терминал" панели навигации интерфейса соответствующего хоста гипервизора (рисунок 28).

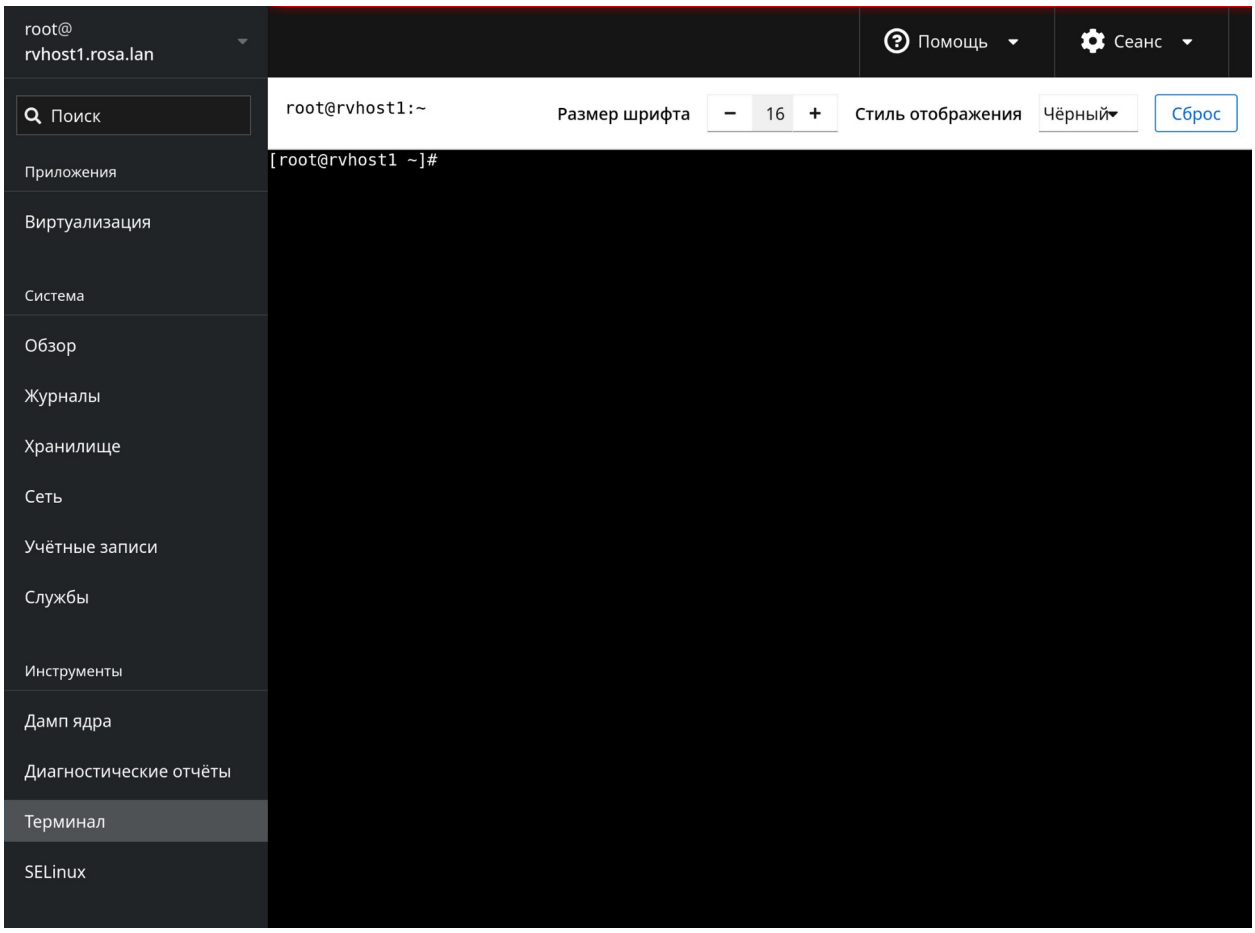

Рисунок 28 – Консоль (терминал) хоста гипервизора, с доступом через веб-интерфейс

3.3.2 Доступ к консоли с использованием SSH

Для доступа к консоли хоста можно воспользоваться SSH-соединением.

Для получения доступа к консоли через SSH используйте имя учетной записи суперпользователя root и пароль, выбранный ранее (см. п.3.2.4.8).

Выполните команду в терминале, указав имя хоста (в примере ниже имя хоста "rvhost1.rosa.lan" замените на имя хоста, развернутого в вашем ЦОД):

```
# ssh root@rvhost1.rosa.lan
```

Примечание – Команды по настройке хоста, указанные в разделах ниже, могут выполняться в консоли с доступом через SSH или в терминале, открытом в браузере веб-интерфейсе администрирования хоста.

3.3.3 Разрешение имен DNS

При отсутствии в сети сервера DNS используйте конфигурационный файл /etc/hosts для настройки разрешения имен DNS в IP-адреса сетевых ресурсов. Конфигурационный файл /etc/hosts содержит построчный список IP-адресов и соответствующих имен DNS для их преобразования при обращении.

3.3.3.1 Редактирование файла /etc/hosts с именами хостов, используемых в системе

В консоли хоста откройте редактор mcedit и укажите в файле /etc/hosts IP-адреса и имена DNS взаимодействующих компонентов ROSA Virtualization – хостов с установленными гипервизорами, ВМ СУСВ и сервера IPA.

Для начала редактирования файла /etc/hosts с использованием редактора mcedit выполните команду в консоли:

```
# mcedit /etc/hosts
```

После завершения редактирования выйдите из редактора, сохранив результат. Для выхода из редактора можно использовать кнопку `Esc`. Если в файл были внесены изменения, то вам предложат их сохранить или выйти без сохранения. Выберите опцию "Сохранить при выходе" – "Да" для сохранения внесенных изменений при выходе из редактора.

Примечания

1) Для сохранения результатов редактирования файла в редакторе mcedit нажмите `F2`. Для выхода из редактора нажмите `F10`. При использовании редактора в окне браузера вы можете нажать на кнопки `F2` и `F10`, используя курсор мыши и левую клавишу мыши.

2) Вы также можете использовать для редактирования любой другой текстовый редактор, например vi.

Для редактирования файла с использованием редактора vi выполните команду:

```
# vi /etc/hosts
```

Для выхода из редактора vi необходимо использовать команду `:q`.

Для перехода в режим редактирования в редакторе vi (режим "INSERT") нажмите клавишу `Insert`. После внесения необходимых изменений нажмите клавишу `Esc`, затем введите команду `:x`.

Ознакомиться подробнее с командами текстового редактора vi вы можете в инструкции к данному тестовому редактору.

Пример файла /etc/hosts с IP-адресами и именами DNS взаимодействующих компонентов ROSA Virtualization – хостов с установленными гипервизорами, ВМ СУСВ и сервера IPA:

```
    10.10.20.4    susv      susv.rosa.lan       # ВМ СУСВ
    10.10.20.6    host1          rvhost1.rosa.lan        #
хост гипервизора
    10.10.20.7    host2          rvhost2.rosa.lan        #
хост гипервизора
    10.10.20.8    host3          rvhost3.rosa.lan        #
хост гипервизора
    10.10.20.9    ipa       ipa.rosa.lan        # сервер IPA
```

Повторите процедуру редактирования файла /etc/hosts на каждом из хостов с установленным гипервизором.

Примечания

1) Указанные в тексте выше IP-адреса СУСВ, хостов виртуализации, сервера IPA являются примером. Используйте для создания конфигурационных файлов IP-адреса СУСВ, хостов, сервера IPA, используемые (заданные) при установке соответствующих хостов в вашем ЦОД.

2) Указание в файле /etc/hosts IP-адресов и имен DNS взаимодействующих компонентов ROSA Virtualization позволяет обеспечить функционирование системы при недоступном корпоративном DNS сервере.

3.3.4 Настройка аутентификации с применением криптографических ключей вместо пароля

Для использования аутентификации с применением криптографических ключей вместо пароля при взаимодействии между хостами с установленными гипервизорами создайте на каждом хосте закрытый и открытый ключи SSH, а затем скопируйте открытый ключ на другие хосты.

3.3.4.1 Создание ключей SSH

Для создания ключей SSH выполните следующую консольную команду:

```
    # ssh-keygen -t rsa
```

При создании ключей рекомендуется принимать предложенные значения параметров по умолчанию. Для этого при выводе запросов нажимайте клавишу `Enter`.

3.3.4.2 Копирование открытых криптографических ключей на другие хосты

После создания ключей скопируйте открытый ключ на другие хосты. Для этого выполняйте следующую команду последовательно указывая имена всех необходимых хостов:

```
# ssh-copy-id имя_хоста
```

В качестве "имя_хоста" в команде выше укажите полное доменное имя хоста, на который надо скопировать открытый ключ с данного хоста.

3.3.4.3 Настройка взаимодействия хоста с системой хранения данных

Для настройки взаимодействия хоста с системой хранения данных выполните в консоли хоста следующие команды:

```
# cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
# ssh -o "StrictHostKeyChecking no" root@`hostname` exit
```

Примечание – При выполнении последней команды переменная "hostname" будет автоматически заменена на действительное имя хоста.

Результат выполнения указанных выше команд в консоли хоста:

```
[root@rvhost1 ~]# cat ~/.ssh/id_rsa.pub >>
~/.ssh/authorized_keys
[root@rvhost1 ~]# ssh -o "StrictHostKeyChecking no"
root@`hostname` exit
Warning: Permanently added "rvhost1.rosa.lan,10.10.20.6"
(GOST) to the list of known hosts.
```

Повторите процедуры создания ключей SSH, копирования открытого ключа и настройки взаимодействия по SSH с системой хранения данных на каждом из хостов с установленным гипервизором.

3.4 Подготовка системы хранения данных

В качестве системы хранения данных ROSA Virtualization может использоваться существующий корпоративный сервер или специально развернутое хранилище одного из следующих типов:

– Gluster;
– NFS;

– iSCSI;
– Ceph.

Развертывание хранилища Gluster осуществляется через веб-интерфейс хоста непосредственно в процессе гиперконвергентной инсталляции СУСВ (см. п. 3.5.1).

Примечание – Хранилище типа NFS, iSCSI или Ceph должно быть подготовлено заранее перед установкой СУСВ.

3.4.1 Подготовка хранилища NFS с использованием веб-интерфейса

Для успешного функционирования платформы виртуализации необходимо создать файловое хранилище или использовать уже имеющееся хранилище.

В данном разделе мы рассмотрим создание файлового хранилища NFS на основе хоста гипервизора.

Откройте в панели управления секцию "Виртуализация" (рисунок 29).

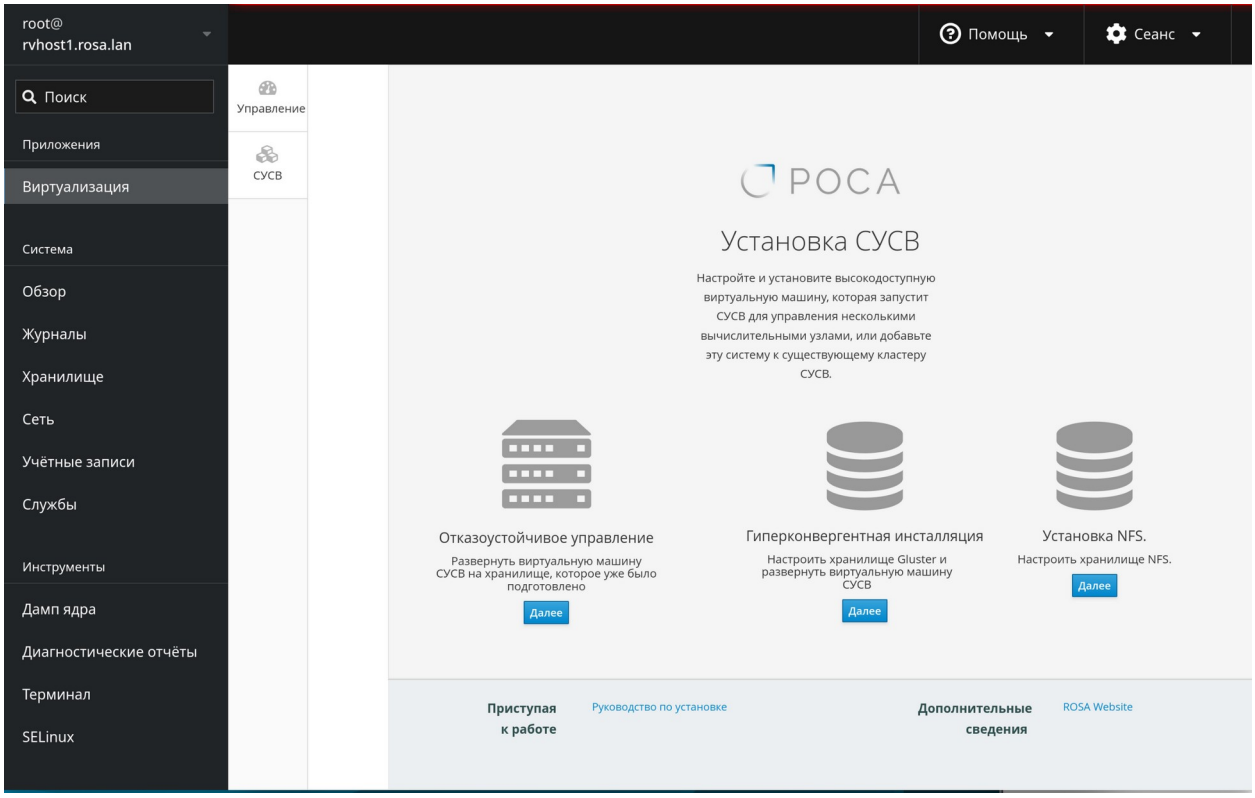

Рисунок 29 – Интерфейс модуля установки СУСВ и настройки файлового хранилища

Выберите в интерфейса секцию "Установка NFS" и нажмите на кнопку Далее.

Откроется диалоговое окно для настройки файлового хранилища NFS (рисунок 30).

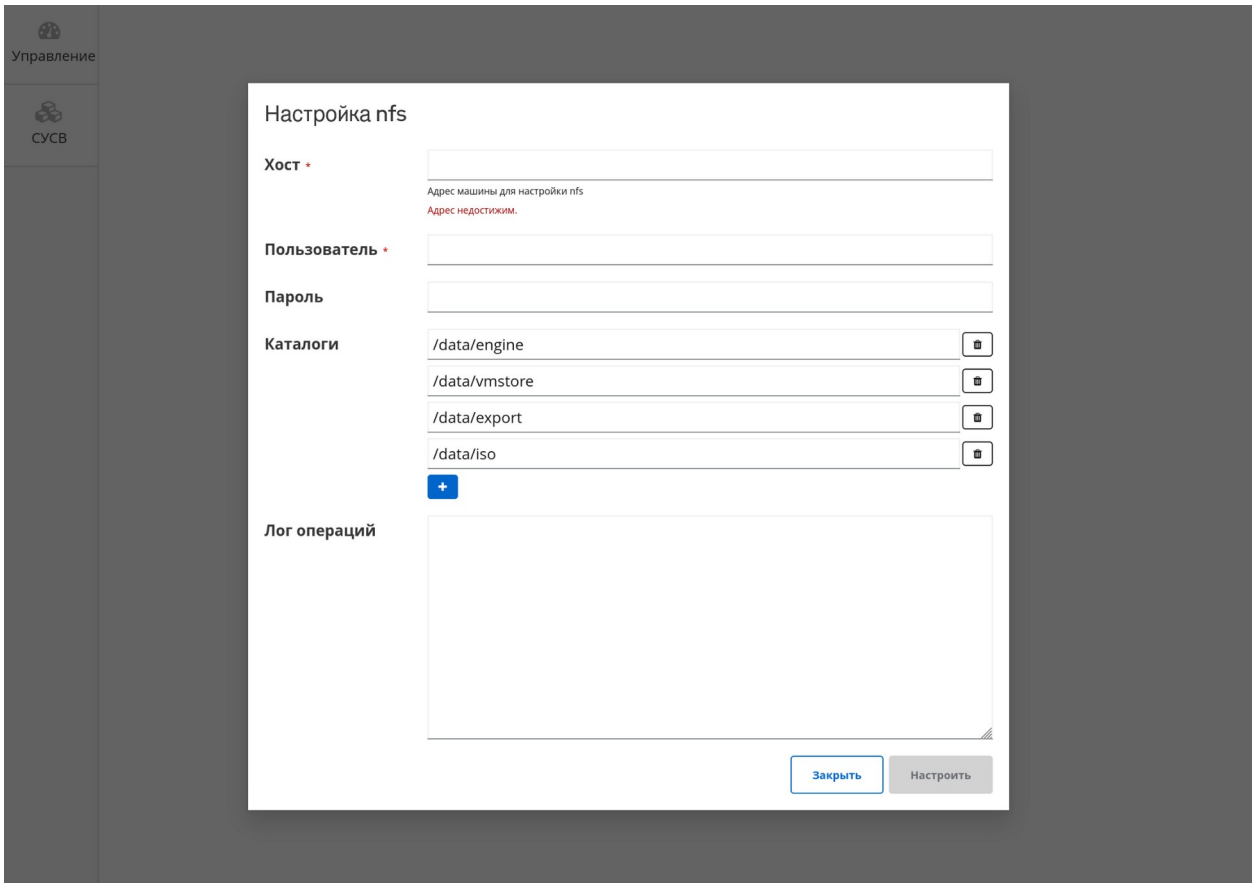

Рисунок 30 – Интерфейс окна для настройки хранилища NFS

Для настройки хранилища NFS вам потребуется имя хоста, имя и пароль пользователя, имеющего права суперпользователя, и структура каталогов (предлагается использовать структуру по умолчанию) (рисунок 31).

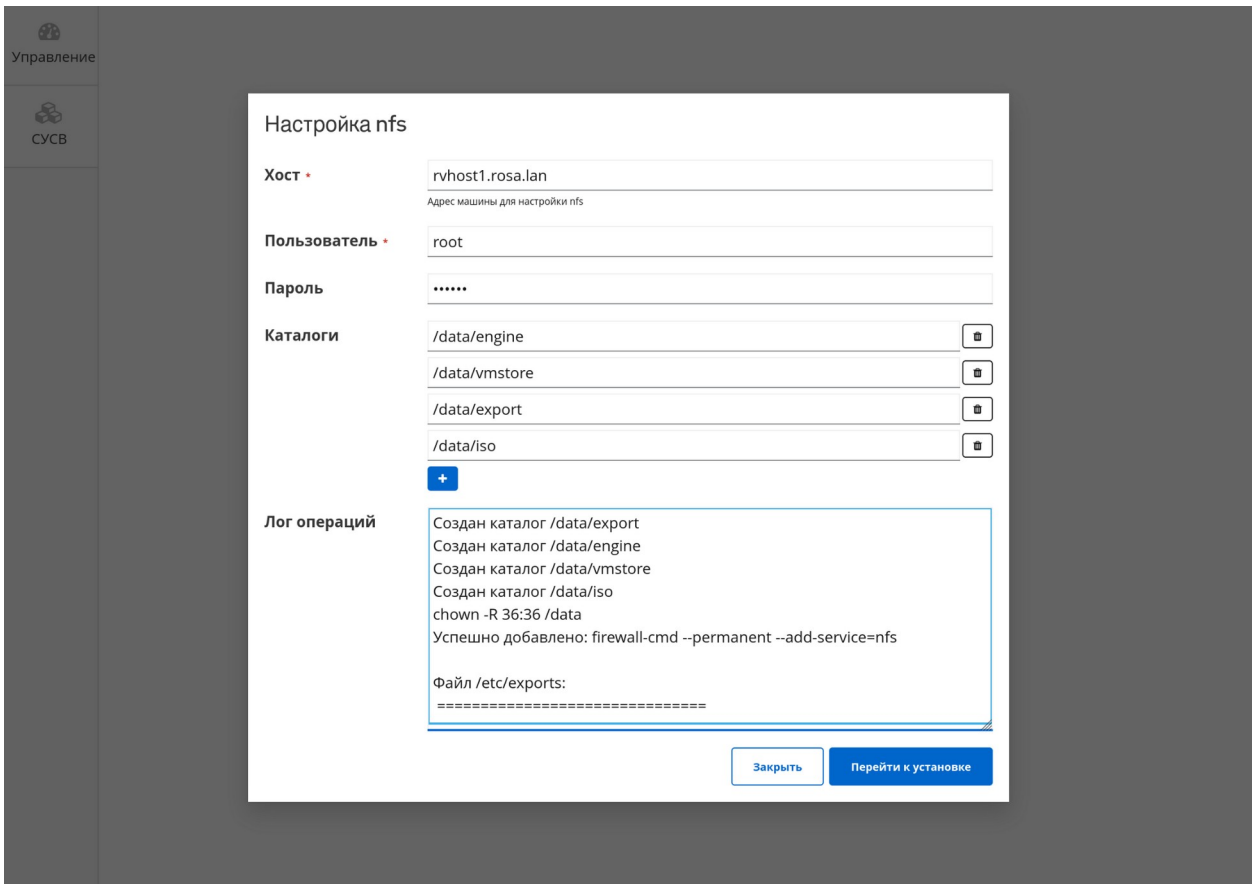

Рисунок 31 – Интерфейс окна для настройки хранилища NFS с указанным именем хоста, логином и лог выполненных действий

После ввода требуемых параметров хранилище NFS будет создано и настроено, в форму "Лог операций" будет выведен лог выполненных действий.

После завершения настройки хранилища NFS можно перейти к установке СУСВ (кнопка `Перейти к установке`) или закрыть форму (кнопка `Закрыть`).

3.4.1.1 Проверка работоспособности NFS хранилища

При необходимости вы можете проверить работоспособность хранилища NFS, выполнив в консоли хоста команду `systemctl status nfs-server` :

```
# systemctl status nfs-server
● nfs-server.service - NFS server and services
   Loaded: loaded (/usr/lib/systemd/system/nfs-
server.service; enabled; vendor preset: disabled)
  Drop-In: /run/systemd/generator/nfs-server.service.d
           └─order-with-mounts.conf
```

```
       Active: active (exited) since Thu 2025-02-27 18:22:15
MSK; 57s ago
      Process: 16131 ExecReload=/usr/sbin/exportfs -r
(code=exited, status=0/SUCCESS)
     Main PID: 15710 (code=exited, status=0/SUCCESS)

    фев 27 18:22:15 rvhost1.rosa.lan systemd[1]: Starting NFS
server and services...
    фев 27 18:22:15 rvhost1.rosa.lan systemd[1]: Started NFS
server and services.
    фев 27 18:22:16 rvhost1.rosa.lan systemd[1]: Reloading NFS
server and services.
    фев 27 18:22:16 rvhost1.rosa.lan systemd[1]: Reloaded NFS
server and services.
```

Статус "Active: active" указывает на то, что сервис активен.

3.4.2 Подготовка хранилища NFS с использованием командной строки

В данном разделе рассматривается подготовка хранилища NFS средствами ROSA Virtualization в консоли хоста, предназначенного для установки ВМ СУСВ.

Примечание – Если вы ранее настроили файловое хранилище NFS с использованием веб-интерфейса, то данную секцию можно пропустить и перейти к следующей.

Для доступа к консоли перейдите на вкладку "Терминал" панели навигации интерфейса соответствующего хоста или откройте консоль хоста через SSH-соединение.

3.4.2.1 Создание структуры каталогов для хранилища NFS

В разделе диска, предназначенном для хранения виртуальных машин и образов, создайте определенную структуру каталогов. Для создания каталогов используйте редактор mc или консольную утилиту mkdir.

Например, выполните следующую команду:

```
    # mkdir -p /data/engine /data/vmstore /data/export /data/iso
```

Измените владельца всех созданных каталогов на служебного пользователя vdsm (uid=36) и соответствующую служебную группу kvm (gid=36). Для этого выполните следующую команду:

```
# chown -R 36:36 /data
```

В редакторе mc (запуск редактора осуществляется из командной строки терминала командой `mcedit`) отредактируйте конфигурационный файл сервера NFS /etc/exports так, чтобы предоставить всем хостам в сети доступ к созданным каталогам на чтение и запись. Для этого добавьте в файл /etc/exports строки следующего содержания:

```
/data/engine   *(rw)
/data/vmstore  *(rw)
/data/export   *(rw)
/data/iso      *(rw)
```

3.4.2.2 Настройка межсетевого экрана для работы с хранилищем NFS

Для разрешения входящих соединений к NFS через службу межсетевого экрана firewalld выполните следующую команду:

```
# firewall-cmd --permanent --add-service=nfs
```

Для применения изменений перезагрузите конфигурацию межсетевого экрана. Для этого выполните следующую консольную команду:

```
# firewall-cmd --reload
```

3.4.2.3 Запуск сервера NFS и настройка автоматического запуска при загрузке системы

По умолчанию сервер NFS не запускается автоматически при загрузке системы.

Для текущего и автоматического запуска сервера NFS при загрузке системы выполните следующие команды:

```
# systemctl start nfs-server
# systemctl enable nfs-server
```

Примечание – При ранее запущенном сервере NFS для применения изменений, внесенных в конфигурацию через редактирование параметров файла /etc/exports, выполните следующую команду:

```
# systemctl reload nfs-server
```

3.4.2.3.1 Проверка работоспособности NFS-сервера

Для проверки статуса NFS-сервера выполните команду:

```
# systemctl status nfs-server
```

Пример выполнения команды по проверке статуса NFS-сервера:

```
# systemctl status nfs-server
● nfs-server.service - NFS server and services
   Loaded: loaded (/usr/lib/systemd/system/nfs-
server.service; enabled; vendor preset: disabled)
  Drop-In: /run/systemd/generator/nfs-server.service.d
           └─order-with-mounts.conf
   Active: active (exited) since Thu 2025-02-27 18:22:15
MSK; 57s ago
  Process: 16131 ExecReload=/usr/sbin/exportfs -r
(code=exited, status=0/SUCCESS)
 Main PID: 15710 (code=exited, status=0/SUCCESS)

фев 27 18:22:15 rvhost1.rosa.lan systemd[1]: Starting NFS
server and services...
фев 27 18:22:15 rvhost1.rosa.lan systemd[1]: Started NFS
server and services.
фев 27 18:22:16 rvhost1.rosa.lan systemd[1]: Reloading NFS
server and services.
фев 27 18:22:16 rvhost1.rosa.lan systemd[1]: Reloaded NFS
server and services.
```

Статус "Active: active" указывает на то, что сервис активен.

3.5 Установка СУСВ

В общем случае установка СУСВ осуществляется через веб-интерфейс хоста (например, "rvhost1.rosa.lan"), на котором будет развернута соответствующая ВМ.

Для выбора одного из вариантов установки СУСВ перейдите на вкладку "Виртуализация" панели навигации интерфейса хоста (рисунок 32). На экране появится меню "Установка СУСВ", в котором способы развертывания СУСВ представлены в виде следующих секций:

– Отказоустойчивое управление;
– Гиперконвергентная инсталляция.

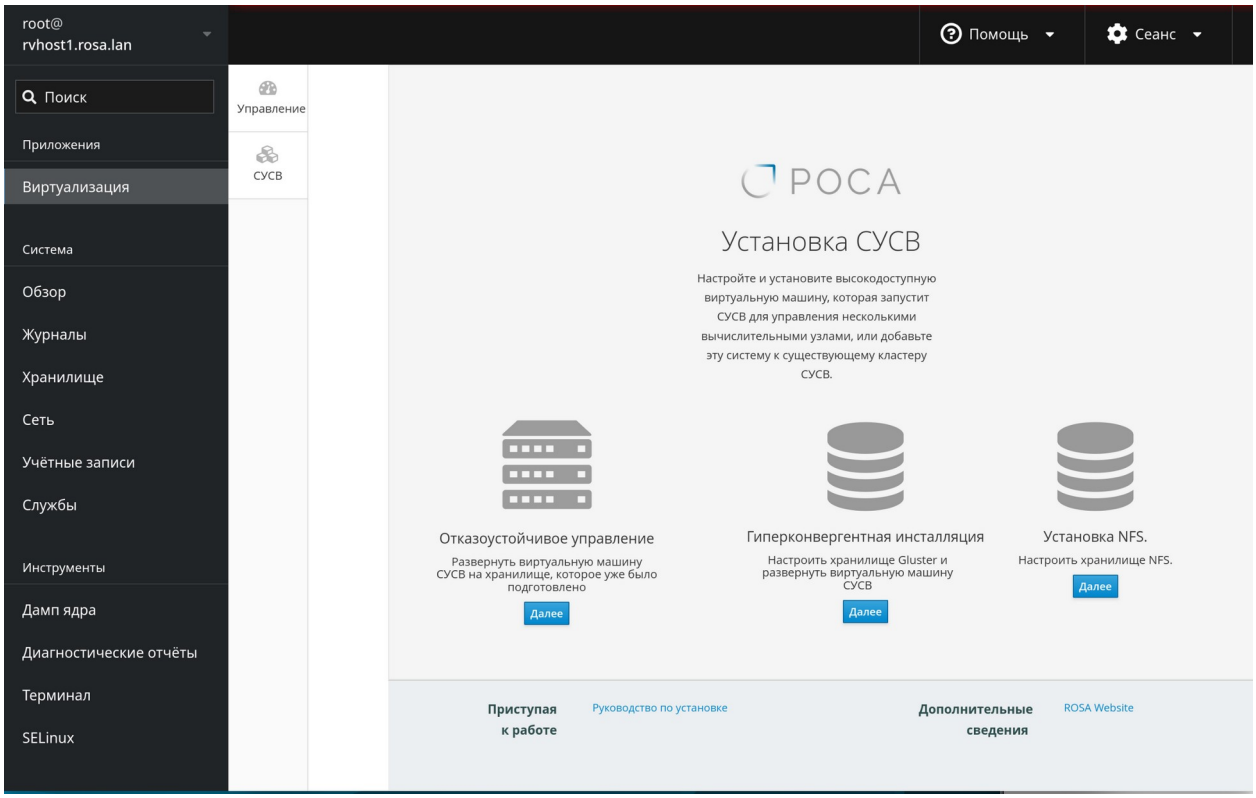

Рисунок 32 – Выбор варианта установки СУСВ в веб-интерфейсе хоста виртуализации

Выбор варианта установки СУСВ:

– Для установки СУСВ на заранее подготовленное хранилище нажмите кнопку Далее в секции "Отказоустойчивое управление". Программа установки запустит интерактивный процесс развертывания ВМ СУСВ (см. п. 3.5.2).

– Для подготовки хранилища Gluster и последующей установки СУСВ в ходе единого процесса нажмите кнопку Далее в секции "Гиперконвергентная инсталляция". Программа установки запустит интерактивный процесс развертывания хранилища Gluster (см. п. 3.5.1).

Примечание – Если вы не планируете использовать хранилище Gluster, то п. 3.5.1 можно пропустить.

3.5.1 Развертывание хранилища Gluster

В окне "Конфигурация Gluster" нажмите кнопку `Запустить установщик Gluster` для перехода к настройке конфигурации хранилища (рисунок 33).

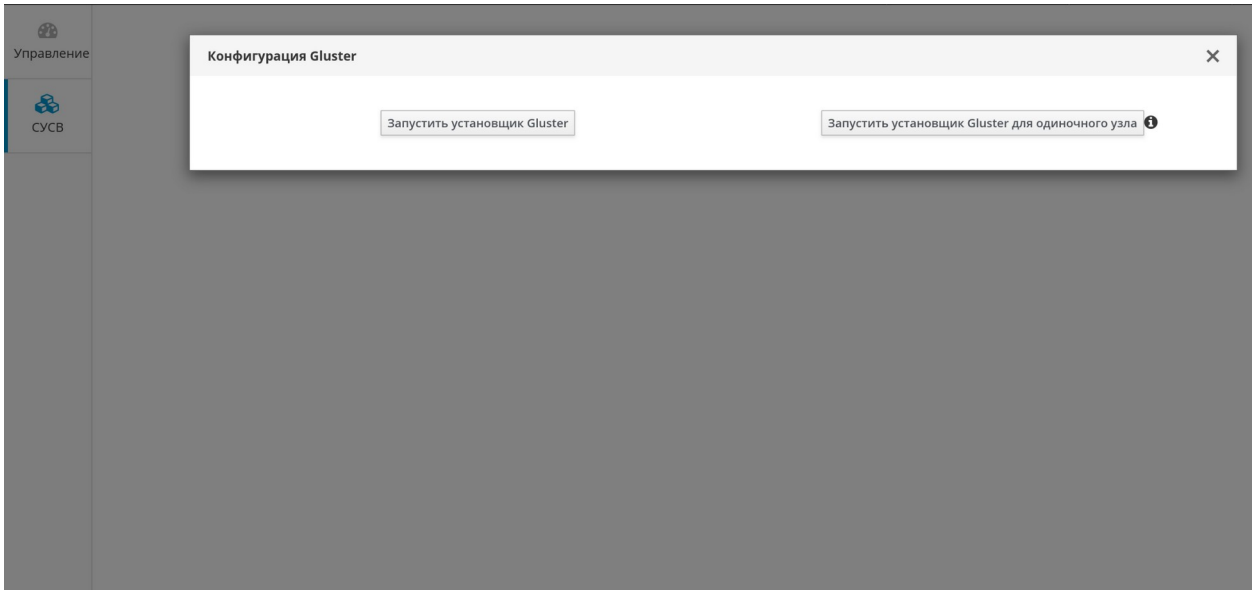

Рисунок 33 – Запуск настройки конфигурации Gluster

Примечание – Если в составе ROSA Virtualization развернут только один хост с установленным гипервизором, то нажмите кнопку `Запустить установщик Gluster для одиночного узла` (рисунок 33). После нажатия кнопки будет запущен установщик Gluster для одиночного узла (рисунок 34)

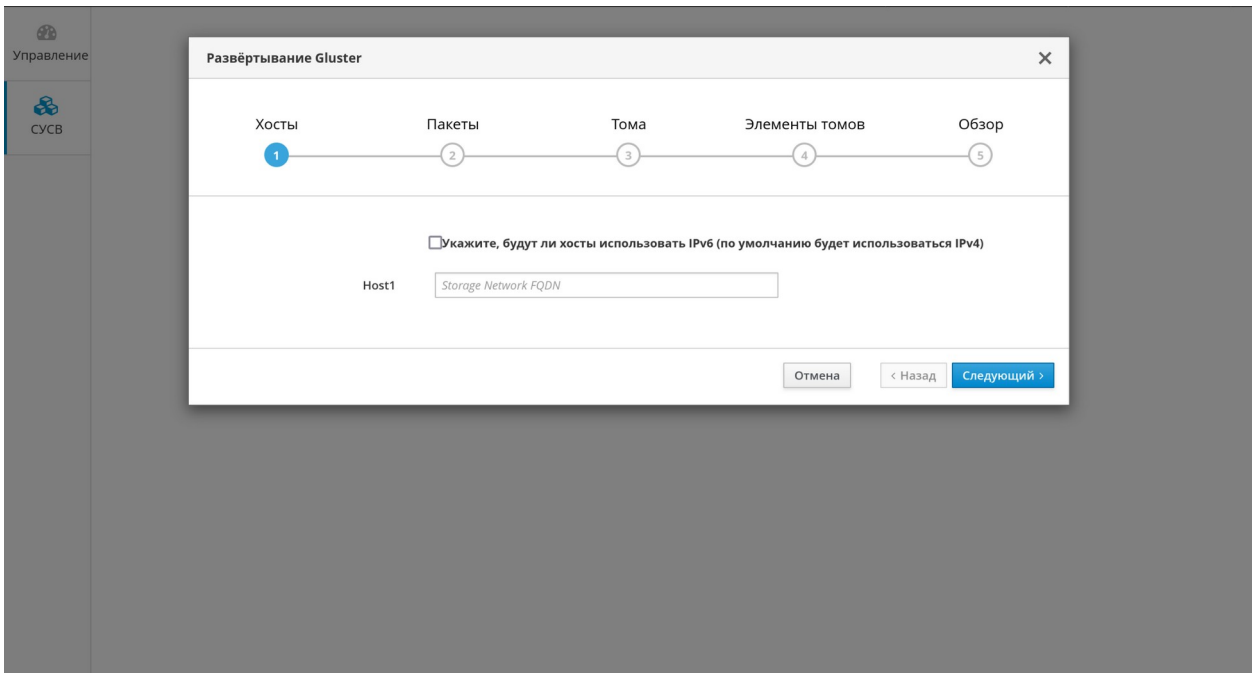

Рисунок 34 – Форма помощника настройки конфигурации Gluster для одиночного узла

3.5.1.1 Настройка конфигурации Gluster для группы из трёх хостов

На экране появится окно "Развертывание Gluster", в котором параметры хранилища распределены по секциям "Хосты", "Пакеты", "Тома", "Элементы томов" и "Обзор" для последовательной настройки конфигурации (рисунок 35).

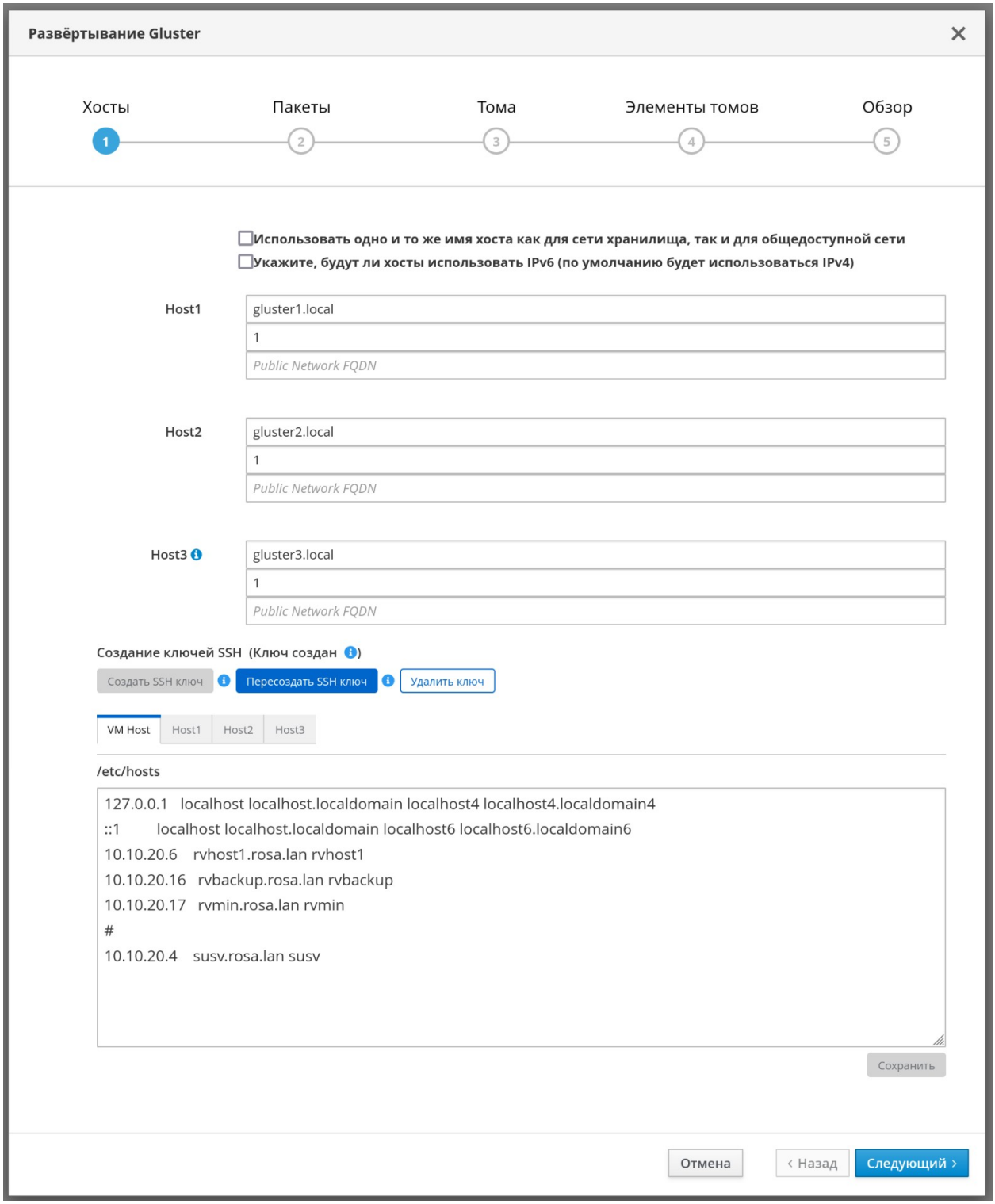

Рисунок 35 – Форма помощника настройки конфигурации Gluster для группы из трех хостов – секция "Параметры хостов"

В секции "Хосты" введите полные доменные имена развернутых хостов ROSA Virtualization в соответствующие поля. При этом хост, указанный в поле

"Host3", будет являться управляющим сервером общего распределенного хранилища Gluster (рисунок 35).

Если указанные имена хостов будут использоваться как для сети хранилища, так и для общедоступной сети, установите соответствующий флажок или отдельно введите имена хостов для общедоступной сети в нижней строке каждого поля.

Для продолжения настройки конфигурации хранилища нажмите кнопку Следующий для перехода к секции "Пакеты" (рисунок 36).

Примечание – В случае появления сообщения об ошибке "Host is not added in known_hosts" выполните процедуру настройки взаимодействия данного хоста с системой хранения данных по SSH (см. п. 3.3.4).

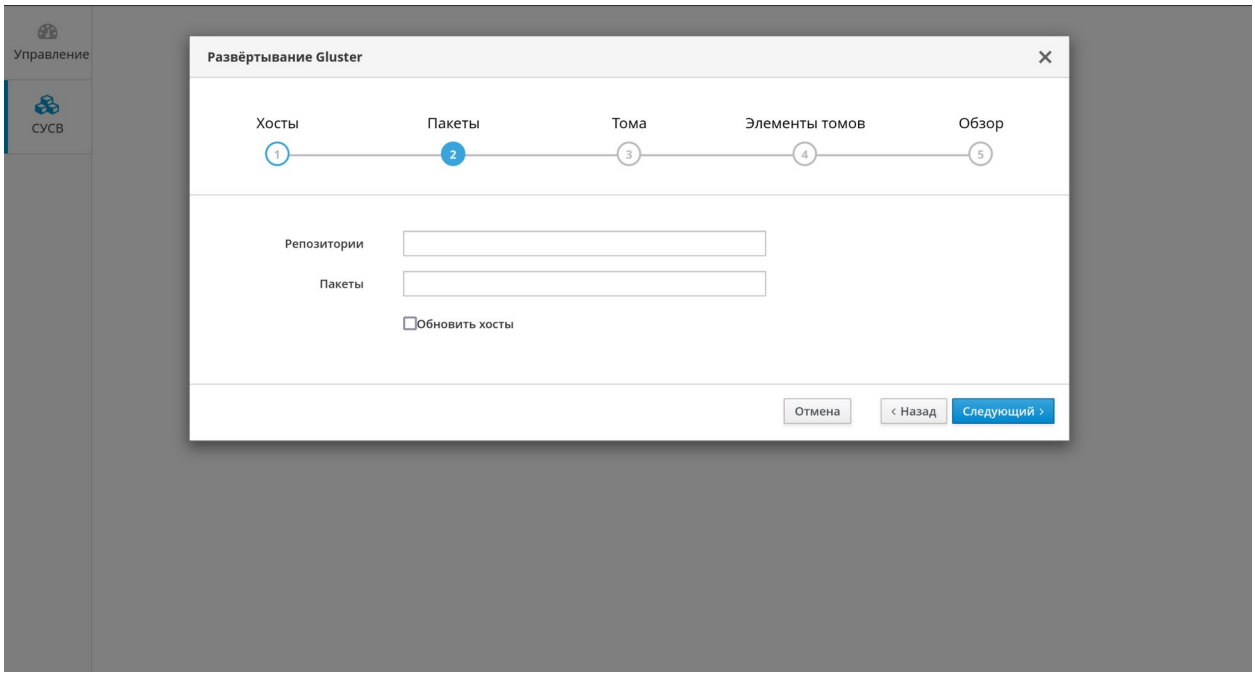

Рисунок 36 – Помощник настройки конфигурации Gluster – секция "Пакеты"

В секции "Пакеты" нажмите кнопку Следующий для продолжения настройки конфигурации хранилища и перехода к секции "Тома" (рисунок 37).

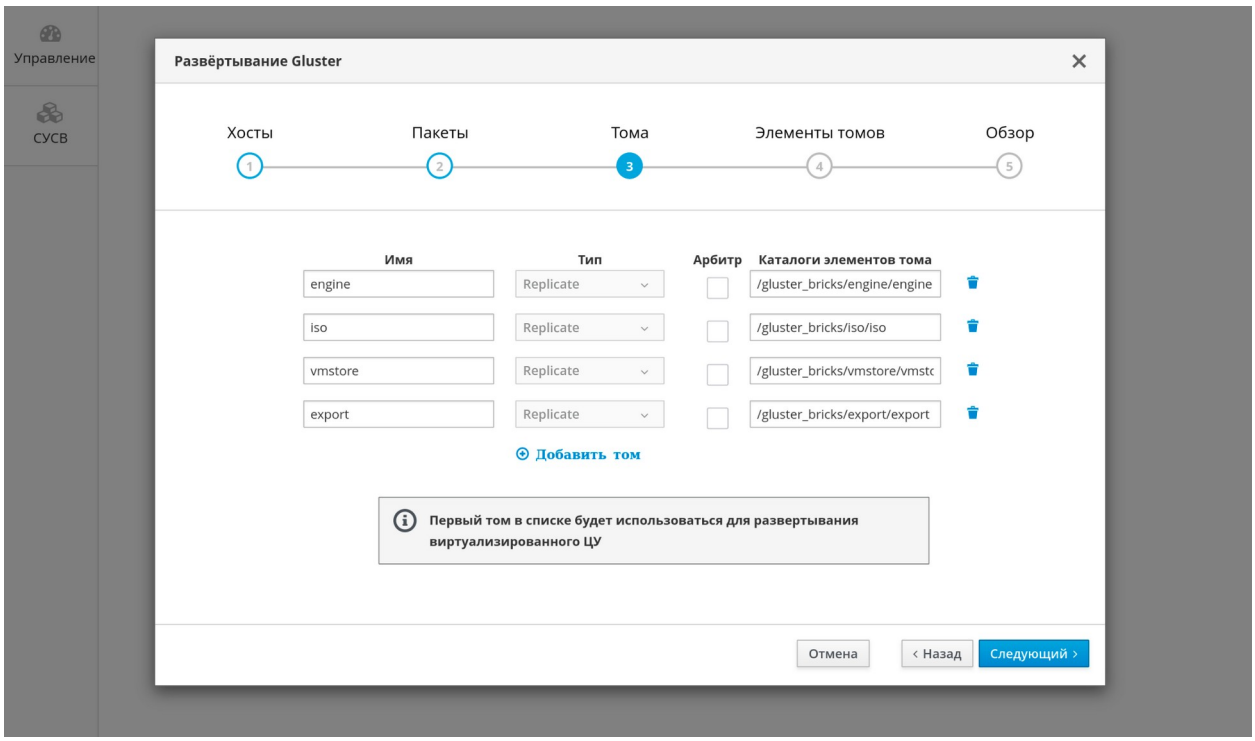

Рисунок 37 – Параметры томов Gluster

В секции "Тома" измените имя тома "data" на значение "iso" и добавьте новый том "export".

Для добавления нового тома нажмите на функциональную строку Добавить том и в поле "Имя" с параметрами нового тома введите значение export.

Примечание – В процессе гиперконвергентной инсталляции корректно настроенным должен быть только домен для хранения виртуальных машин, размещенный на томе vmstore. Параметры остальных томов можно будет отредактировать после завершения установки.

Нажмите кнопку Следующий для продолжения настройки конфигурации хранилища и перехода к секции "Элементы томов" (рисунок 38).

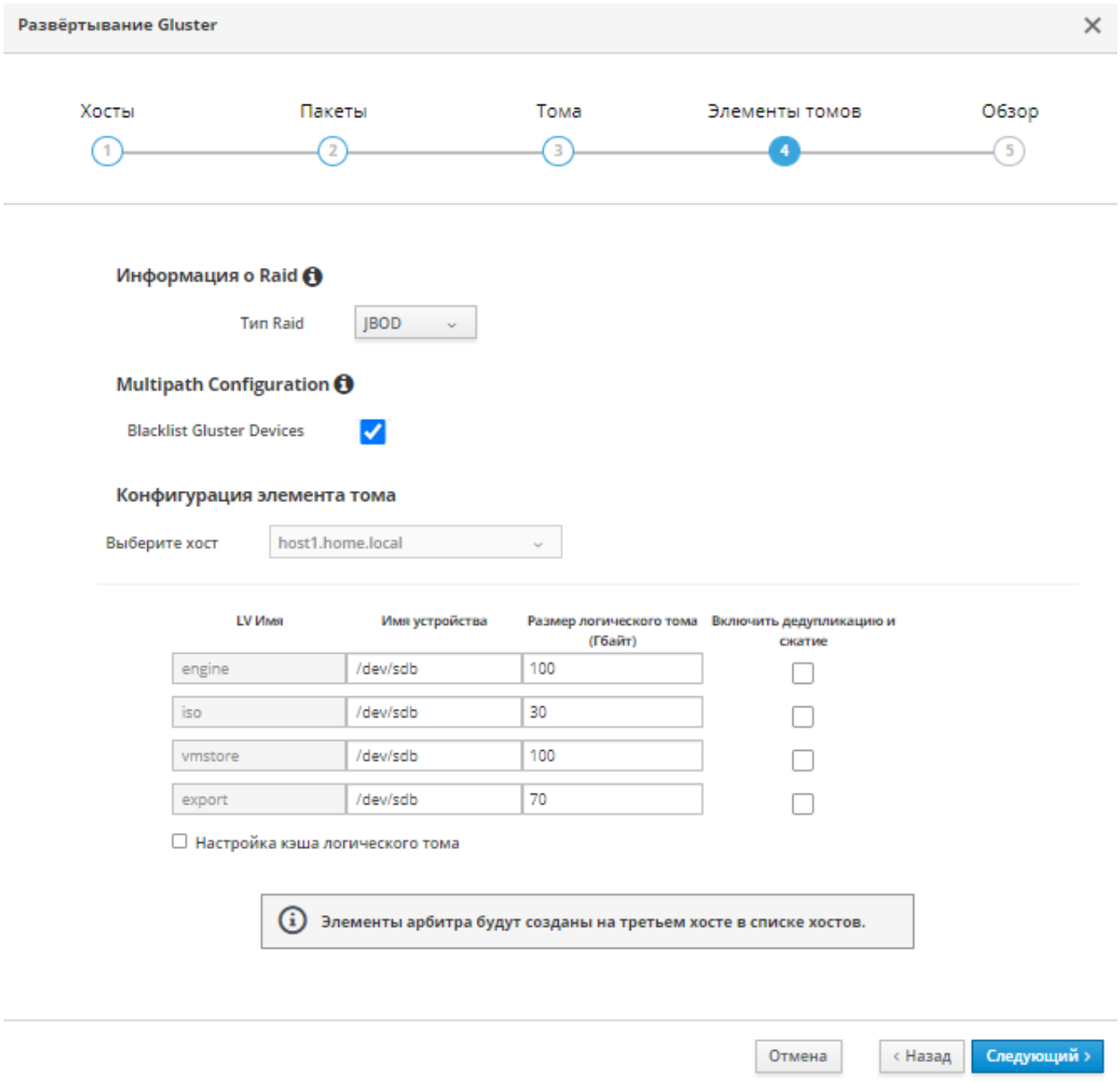

Рисунок 38 – Конфигурация элементов томов Gluster

В секции "Элементы томов" из выпадающего списка "Тип Raid" выберите значение "JBOD", а также при необходимости отредактируйте значения конфигурации элемента для каждого тома.

В графе "Имя устройства" укажите дисковый накопитель (по умолчанию /dev/sdb), предназначенный для развертывания хранилища.

Примечание – Для получения сведений о подключенных к системе накопителях выполните консольную команду `fdisk -l`.

В графе "Размер логического тома (Гбайт)" укажите размер для каждого тома исходя из объема хранилища. При этом размер тома "engine"

должен быть не менее **62 ГБ** свободного дискового пространства для функционирования системы управления.

Примечание – Включать дедупликацию и сжатие томов не рекомендуется.

Нажмите кнопку Следующий для перехода к секции "Обзор" (рисунок 39).

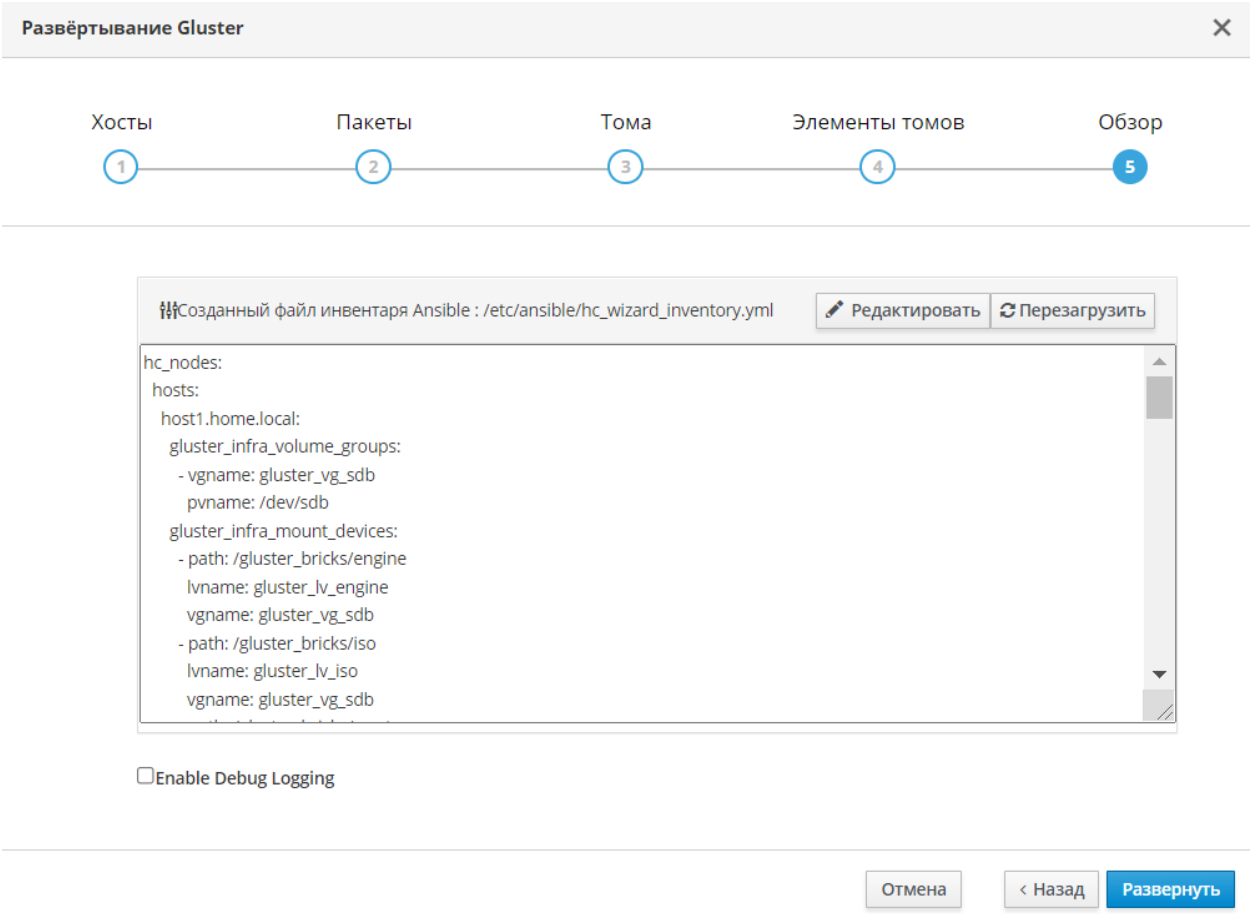

Рисунок 39 – Обзор параметров конфигурации хранилища Gluster

В секции "Обзор" нажмите кнопку Развернуть для подготовки и установки хранилища в соответствии с заданной конфигурацией.

Ход процесса развертывания хранилища будет сопровождаться появлением информационных сообщений о действиях, выполненных программой установки (рисунок 40). В случае неудачной установки можно просмотреть сообщения (в том числе, сообщения об ошибках) для выявления проблемы в процессе установки.

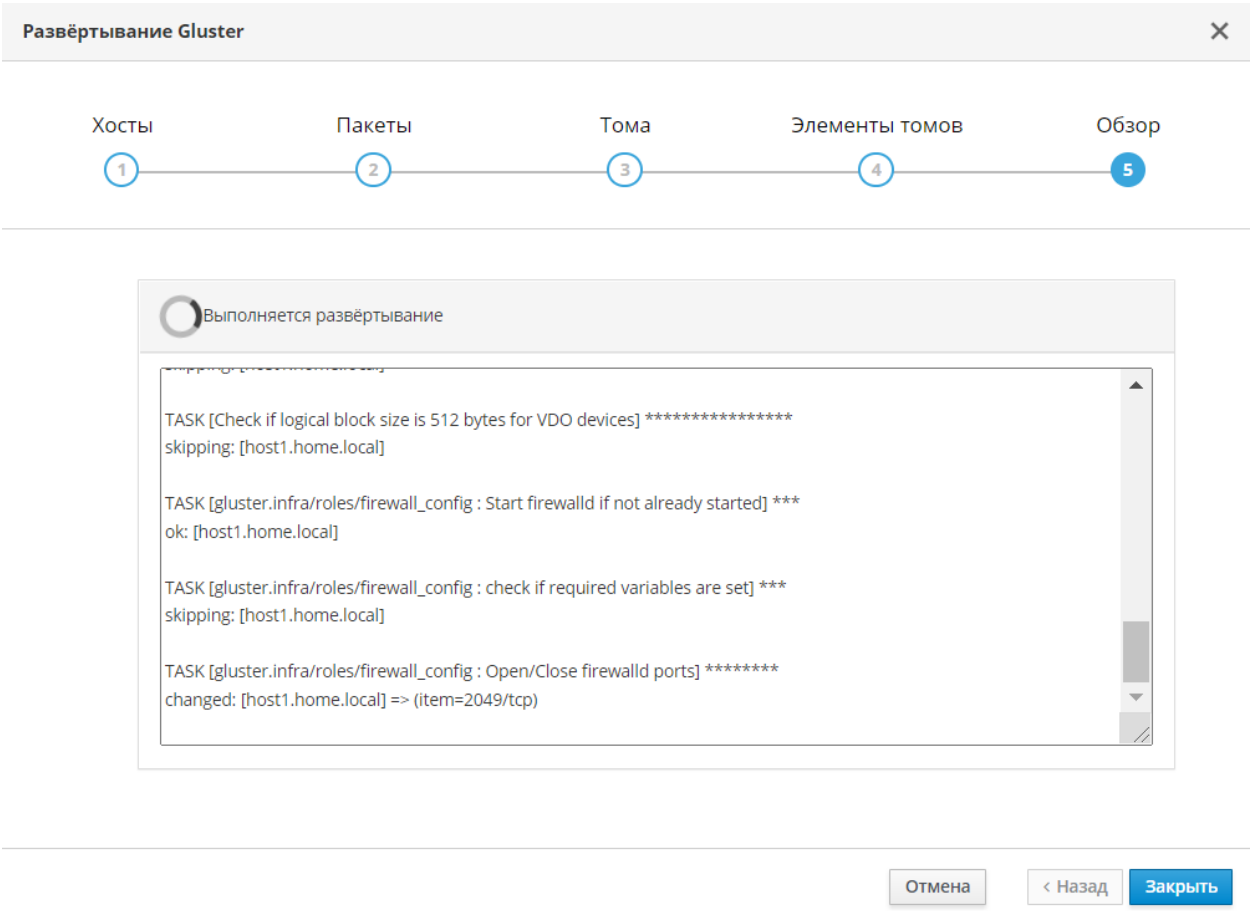

Рисунок 40 – Ход процесса развертывания хранилища Gluster

После успешного завершения процесса развертывания хранилища на экране появится соответствующее сообщение (рисунок 41).

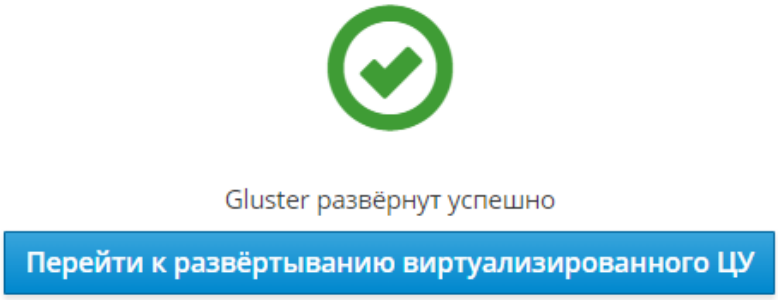

Рисунок 41 – Завершение развертывания хранилища Gluster

Для запуска интерактивного процесса установки ВМ СУСВ на развернутое хранилище Gluster нажмите кнопку `Перейти к развертыванию виртуализированного ЦУ`.

3.5.2 Процесс установки виртуальной машины СУСВ

Перед развертыванием СУСВ программой установки осуществляется предварительная настройка конфигурации.

На экране появится окно "Развертывание виртуализированного ЦУ", в котором параметры СУСВ распределены по секциям "ВМ", "ВиртЦУ", "Подготовка ВМ", "Хранилище" и "Завершить" для последовательной настройки конфигурации.

3.5.2.1 Задание параметров виртуальной машины

На первом этапе развертывания виртуализированного центра управления (ЦУ) осуществляется настройка параметров виртуальной машины, в которой будет развернута СУСВ (рисунок 42).

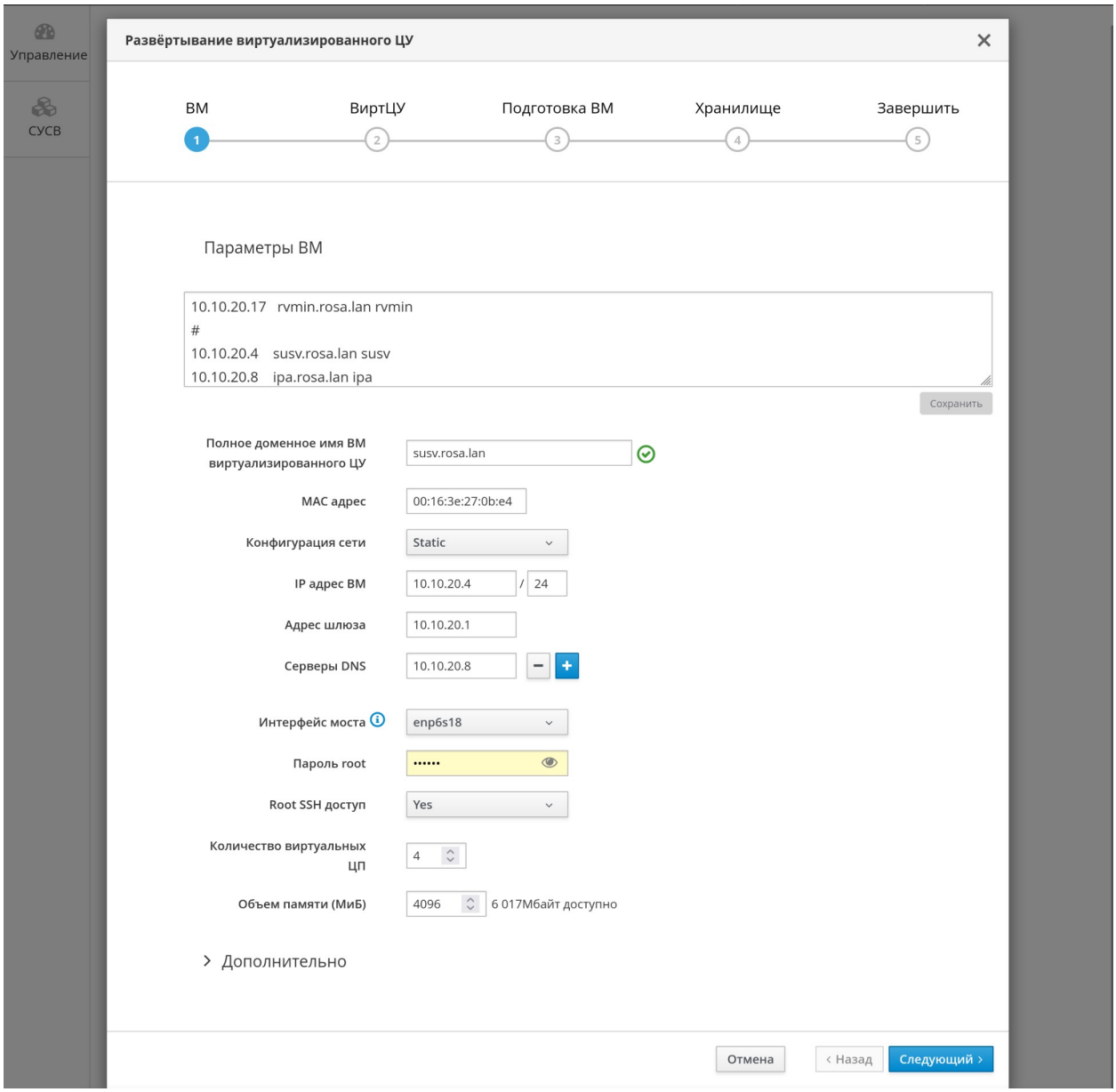

Рисунок 42 – Задание параметров ВМ для развертывания виртуализированного ЦУ

3.5.2.1.1 Редактирование содержимого файла /etc/hosts

В текстовом поле в верхней части формы выводится содержание файла /etc/hosts.

Данное поле является редактируемым. Внесите в него необходимые изменения и сохраните, нажав на кнопку Сохранить (рисунок 43).

Редактирование файла /etc/hosts в веб-интерфейсе установщика виртуализированного ЦУ осуществляется аналогично тому, как описано в п. 3.3.3 и п. 3.3.3.1.

Укажите в форме, соответствующей файлу /etc/hosts, IP-адреса и имена DNS взаимодействующих компонентов ROSA Virtualization – хостов с установленными гипервизорами, ВМ СУСВ и сервера IPA.

После внесения всех необходимых изменений сохраните содержимое в файл /etc/hosts, нажав на кнопку Сохранить (рисунок 43).

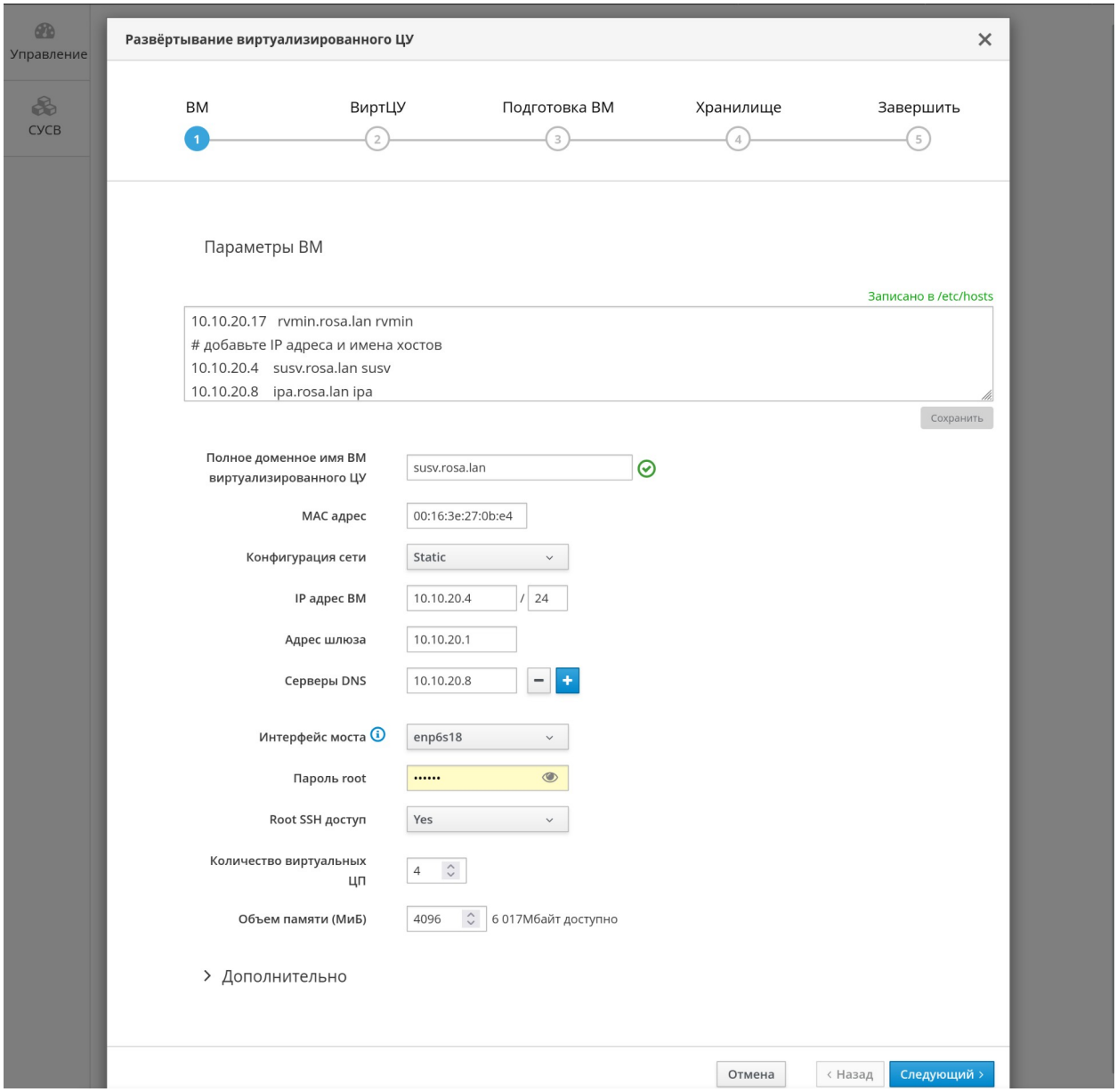

Рисунок 43 – Сохранение содержимого формы в файл /etc/hosts

В секции "Полное доменное имя ВМ виртуализированного ЦУ" задайте полное доменное имя ВМ СУСВ (например, "susv.rosa.lan") в соответствующем поле.

Примечание – Доменное имя ВМ СУСВ должно быть разрешимо с того хоста, с которого осуществляется установка. Если установщик успешно смог разрешить доменное имя, то рядом с данным полем появится значок (рисунок 43). В противном случае вам необходимо предпринять дополнительные шаги для обеспечения разрешения доменного имени.

Из выпадающего списка "Конфигурация сети" выберите необходимое значение – "DHCP" или "Static".

Примечание – Рекомендованный метод указания адресов в конфигурации сети – "Static".

При выборе в конфигурации сети значения "Static" укажите в соответствующих полях:

– IP-адрес ВМ (например, на рисунке 43 – "10.10.20.4"),

– префикс маски подсети – "24",

– адрес шлюза – "10.10.20.1",

– IP-адрес сервера DNS – "10.10.20.8". Для указания дополнительного сервера DNS нажмите кнопку + и введите IP-адрес в новом поле.

– В поле "Пароль root" задайте пароль для учетной записи суперпользователя root ВМ СУСВ.

– В поле "Root SSH доступ" укажите "Yes".

Примечание – Актуальные IP-адреса и маска подсети зависят от используемых параметров вашего сетевого окружения.

При указании значения объема оперативной памяти в соответствующем поле учитывайте, что при развертывании ROSA Virtualization в стартовой конфигурации минимальный объем памяти ВМ СУСВ должен составлять не менее 4096 МБ, а при развертывании в базовой конфигурации – не менее 8192 МБ. При этом системе хоста необходимо дополнительно минимум 512 МБ памяти для функционирования гипервизора.

Примечание – Значение по умолчанию в поле "Количество виртуальных ЦП" изменять не рекомендуется.

3.5.2.1.2 Настройка параметров в секции "Дополнительно"

Нажмите на секцию "Дополнительно" для настройки (при необходимости) дополнительных параметров установки (рисунок 44):

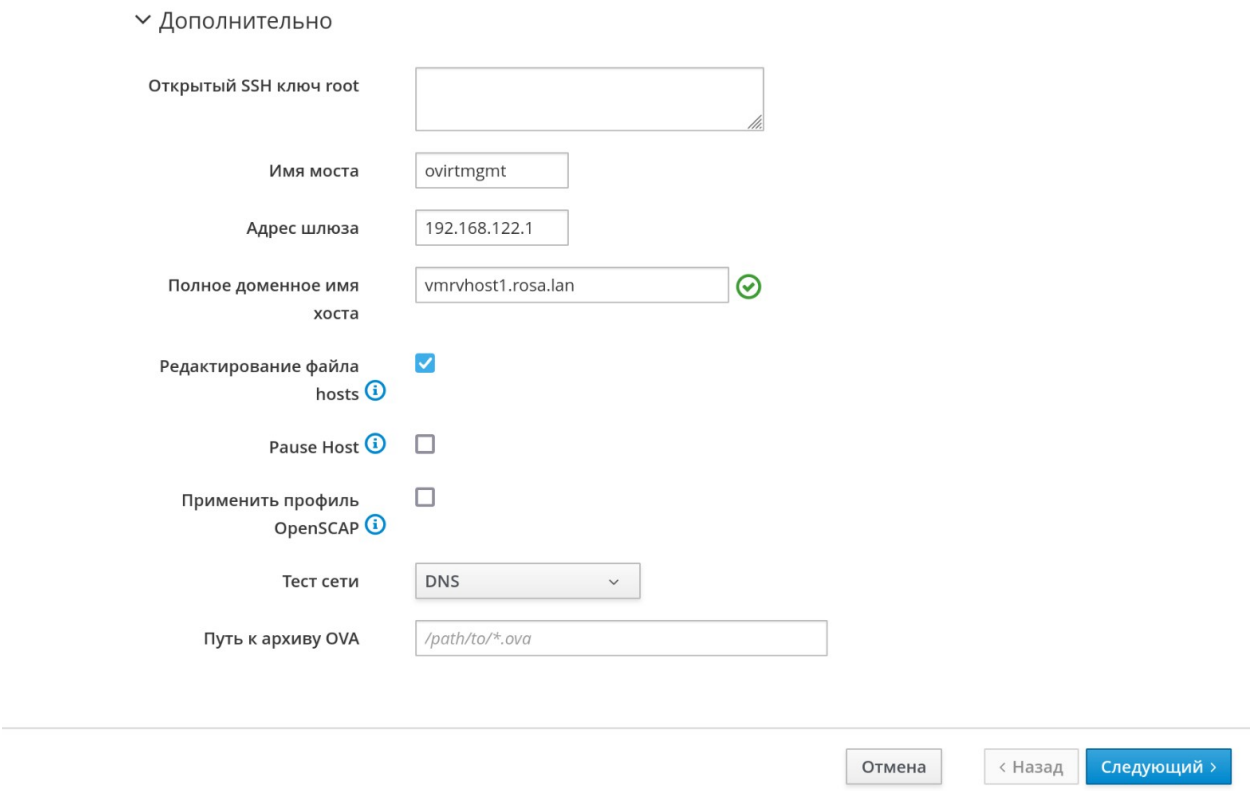

Рисунок 44 – Настройка дополнительных параметров

– Открытый SSH ключ root – параметры открытого ключа SSH для учетной записи администратора (root).

– Имя моста – имя моста, к которому будет подключен СУСВ (изменять не рекомендуется).

– Адрес шлюза – адрес шлюза, используемого СУСВ.

– Полное доменное имя хоста – полное доменное имя хоста. Значок рядом с именем означает, что доменное имя хоста успешно разрешается.

Примечание – Если рядом с именем хоста не отображается значок , то система не может разрешить указанное доменное имя. Проверьте настройки имени хоста в /etc/hosts и внесите необходимые изменения.

– Редактирование файла hosts – добавьте строки с IP-адресом и именем хоста для самого устройства и для этого хоста в файл /etc/hosts на машине виртуализированного ЦУ.

– Pause Host – отметьте эту опцию, если вы хотите приостановить установку, чтобы внести изменения вручную. Это приостановит развертывание после настройки engine (СУСВ) и создаст файл блокировки в директории /tmp, оканчивающийся на "he_setup_lock". Развертывание hosted engine

продолжится после удаления файла блокировки или через 24 часа, если файл не был удален.

– Применить профиль OpenSCAP – применить изначальный профиль защиты OpenSCAP на ВМ виртуализированного ЦУ.

– Тест сети – из опций:

– DNS;
– Ping;
– TCP;
– None;

выберите опцию, каким образом будет осуществляться тестирование сети. При выборе опции "none" тестирование сети осуществляться не будет.

– Путь к архиву OVA – путь к архиву OVA (файл с расширением *.ova). Файл OVA (Open Virtual Appliance) – это каталог OVF, сохраненный в виде архива с использованием формата архивации .tar.

Нажмите кнопку Следующий для продолжения настройки конфигурации СУСВ и перехода к секции "ВиртЦУ".

3.5.2.2 Настройка виртуализированного ЦУ

В секции "ВиртЦУ" задайте пароль для учетной записи admin администратора СУСВ в поле "Пароль Портала администрирования" (рисунок 45).

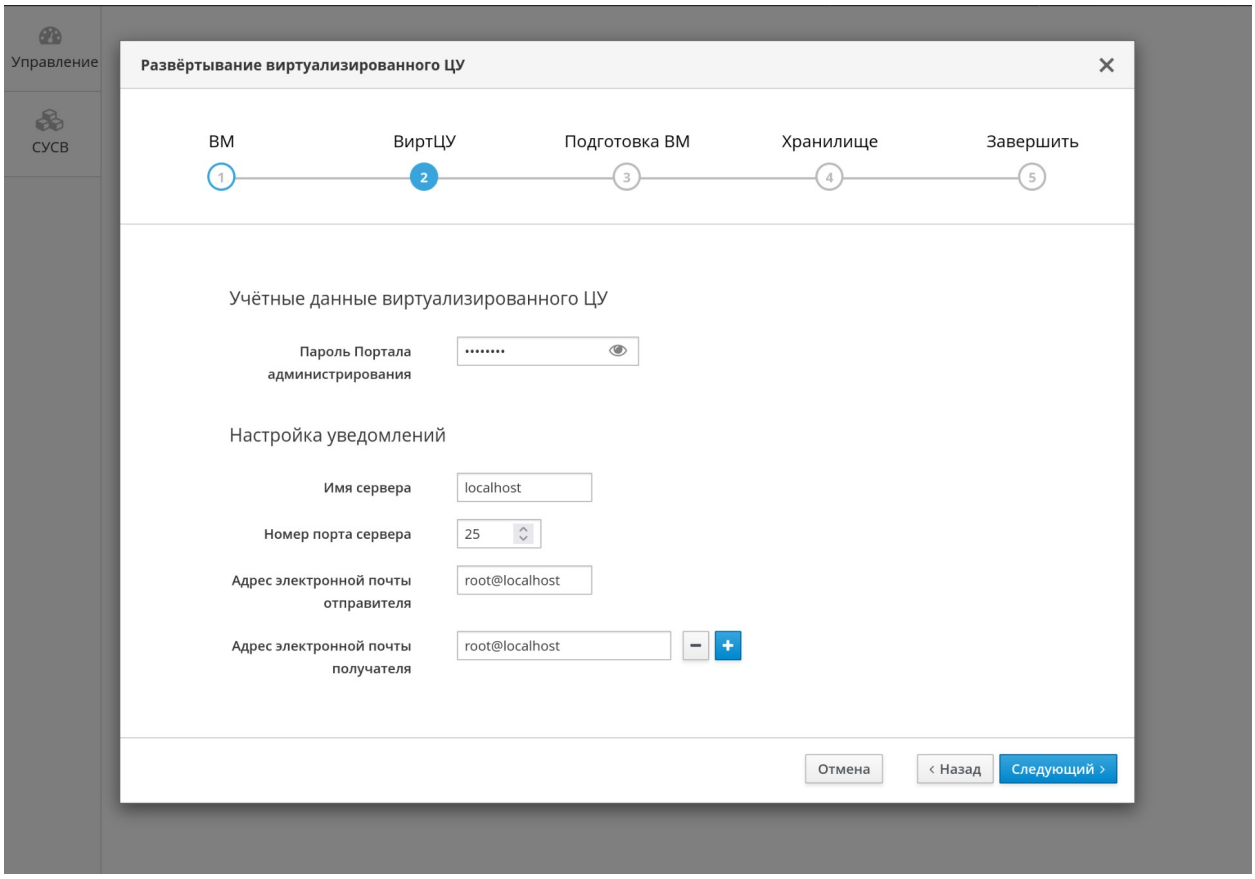

Рисунок 45 – Параметры СУСВ (Виртуального ЦУ)

При необходимости и возможности подключения к внешнему почтовому серверу для настройки уведомлений укажите в соответствующих полях имя и номер порта почтового сервера, а также адреса электронной почты отправителя и получателя.

Нажмите кнопку `Следующий` для перехода к секции "Подготовка ВМ".

3.5.2.3 Подготовка виртуальной машины

В секции "Подготовка ВМ" нажмите кнопку `Подготовить ВМ` для создания и запуска ВМ в соответствии с заданной конфигурацией (рисунок 46).

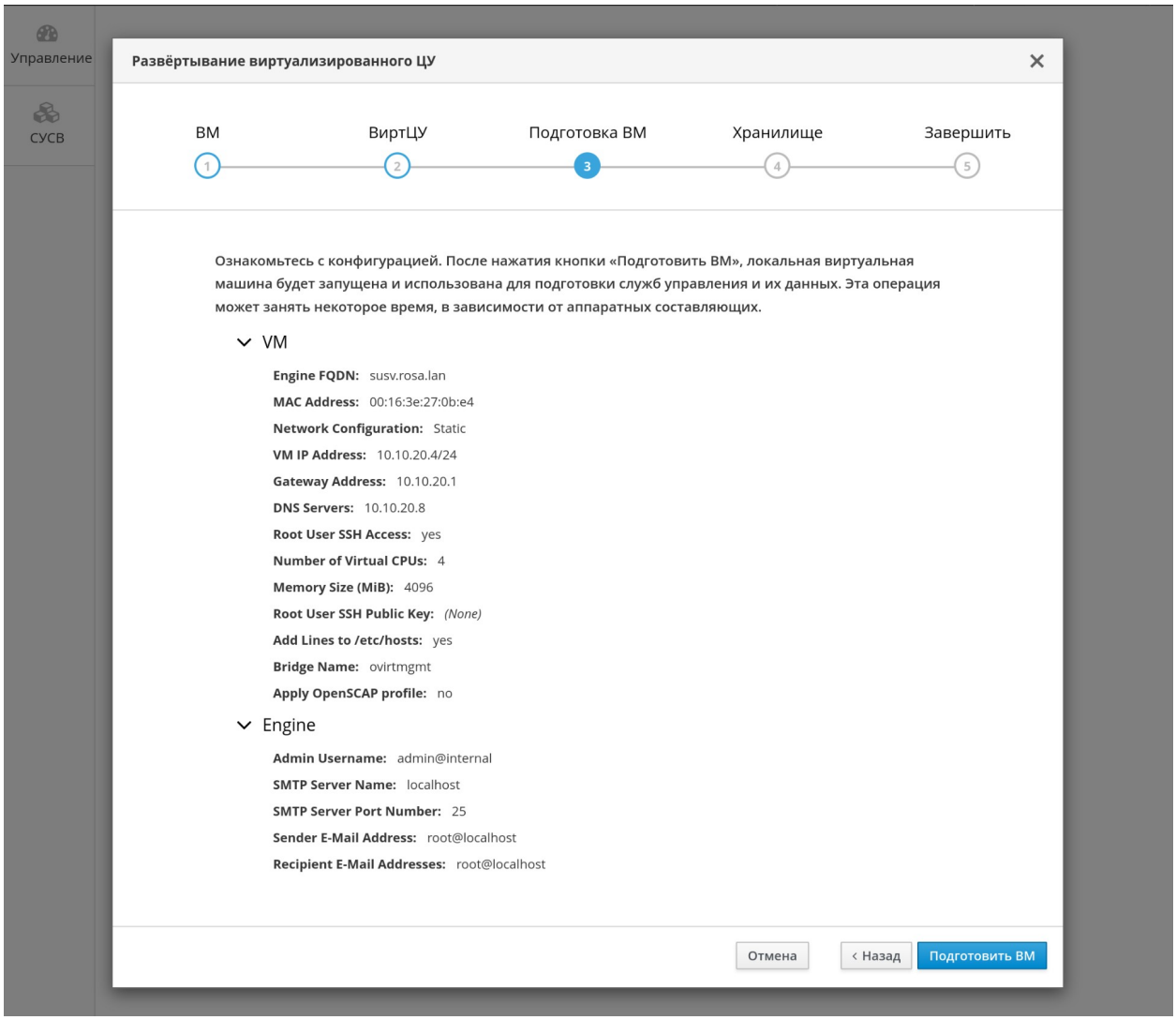

Рисунок 46 – Обзор параметров конфигурации ВМ Виртуального ЦУ (СУСВ)

При необходимости внести изменения в ранее введенные параметры, нажмите на кнопку `< Назад`. Для отмены установки Виртуализированного ЦУ нажмите на кнопку `Отмена`.

После успешного завершения запуска ВМ на экране появится соответствующее сообщение (рисунок 47).

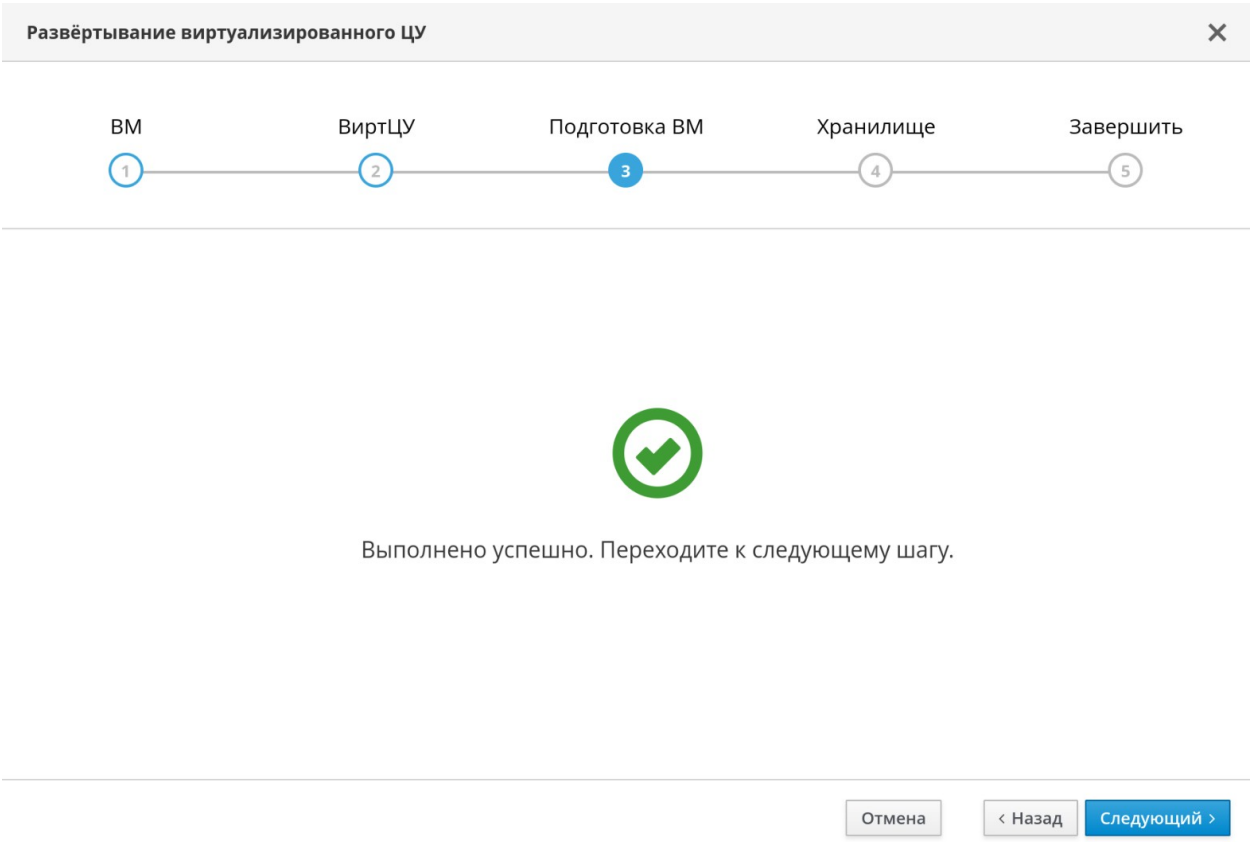

Рисунок 47 – Завершение подготовки ВМ

Нажмите кнопку Следующий для перехода к секции "Хранилище".

3.5.2.4 Настройка параметров хранилища

В секции "Хранилище" выберите из выпадающего списка "Тип хранилища" необходимое значение – "Gluster", "NFS" или "iSCSI" (рисунок 48).

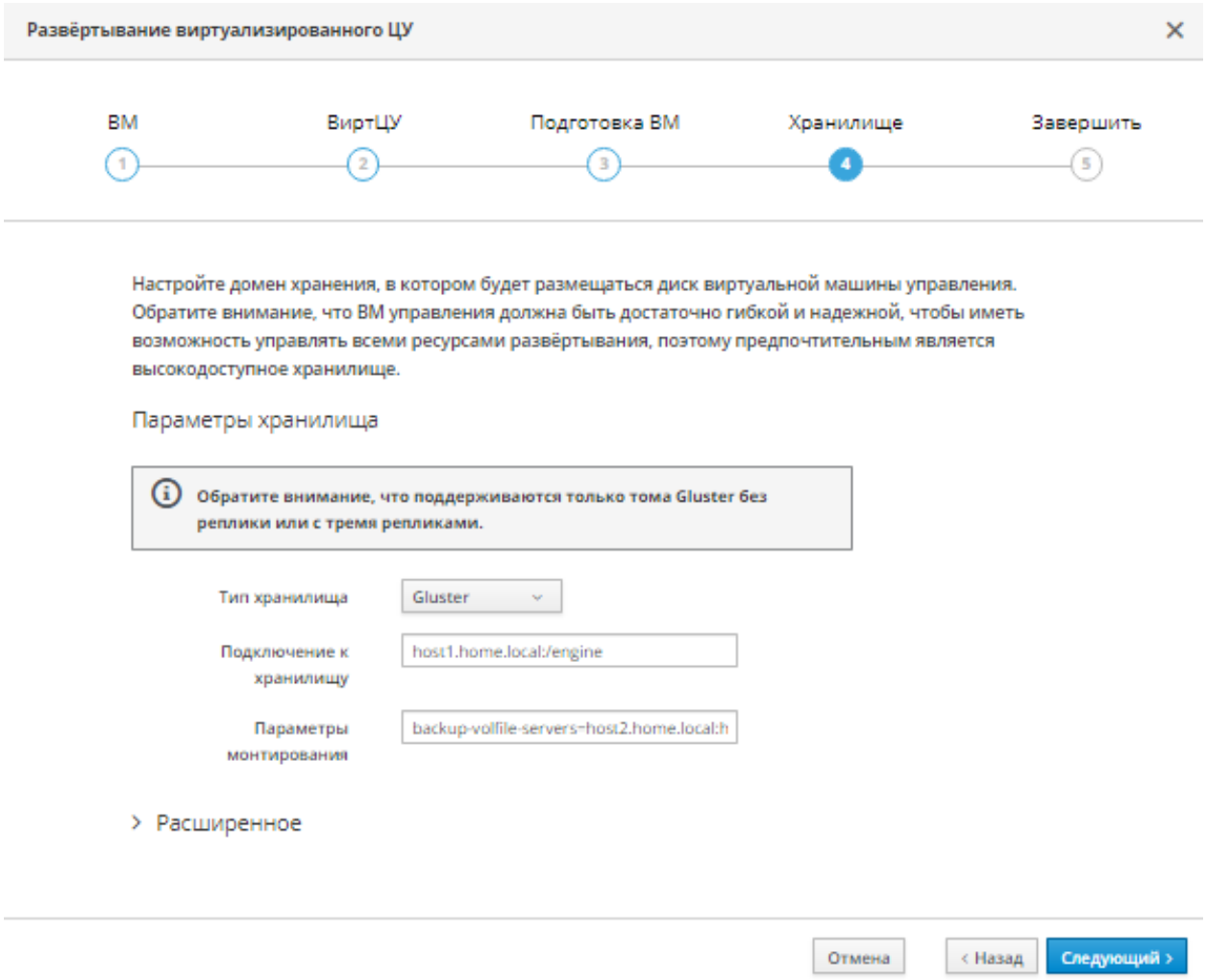

Рисунок 48 – Параметры хранилища типа Gluster

3.5.2.4.1 Настройка хранилища типа Gluster

При выборе типа хранилища Gluster, созданного в п. 3.5.1, укажите в поле "Подключение к хранилищу" том engine (например, rvhost1.rosa.lan:/engine).

3.5.2.4.2 Настройка хранилища типа NFS

При выборе типа хранилища NFS укажите в поле "Подключение к хранилищу" путь к хранилищу (например, rvhost1.rosa.lan:/data/engine), созданному в п. 3.4.1 (рисунок 49).

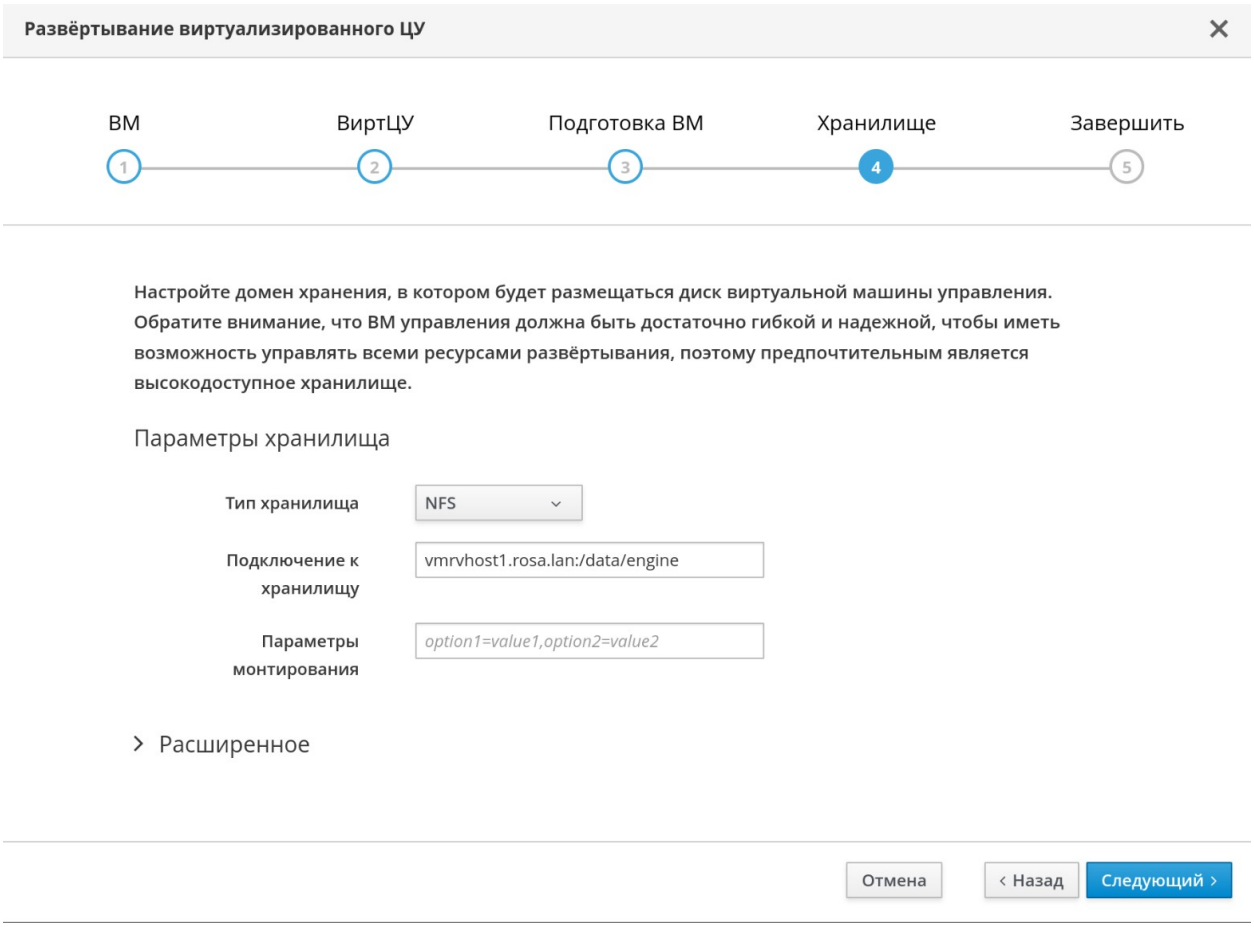

Рисунок 49 – Параметры хранилища типа NFS

3.5.2.4.3 Настройка расширенных параметров

Для настройки расширенных параметров нажмите на "Расширенное" (рисунок 50):

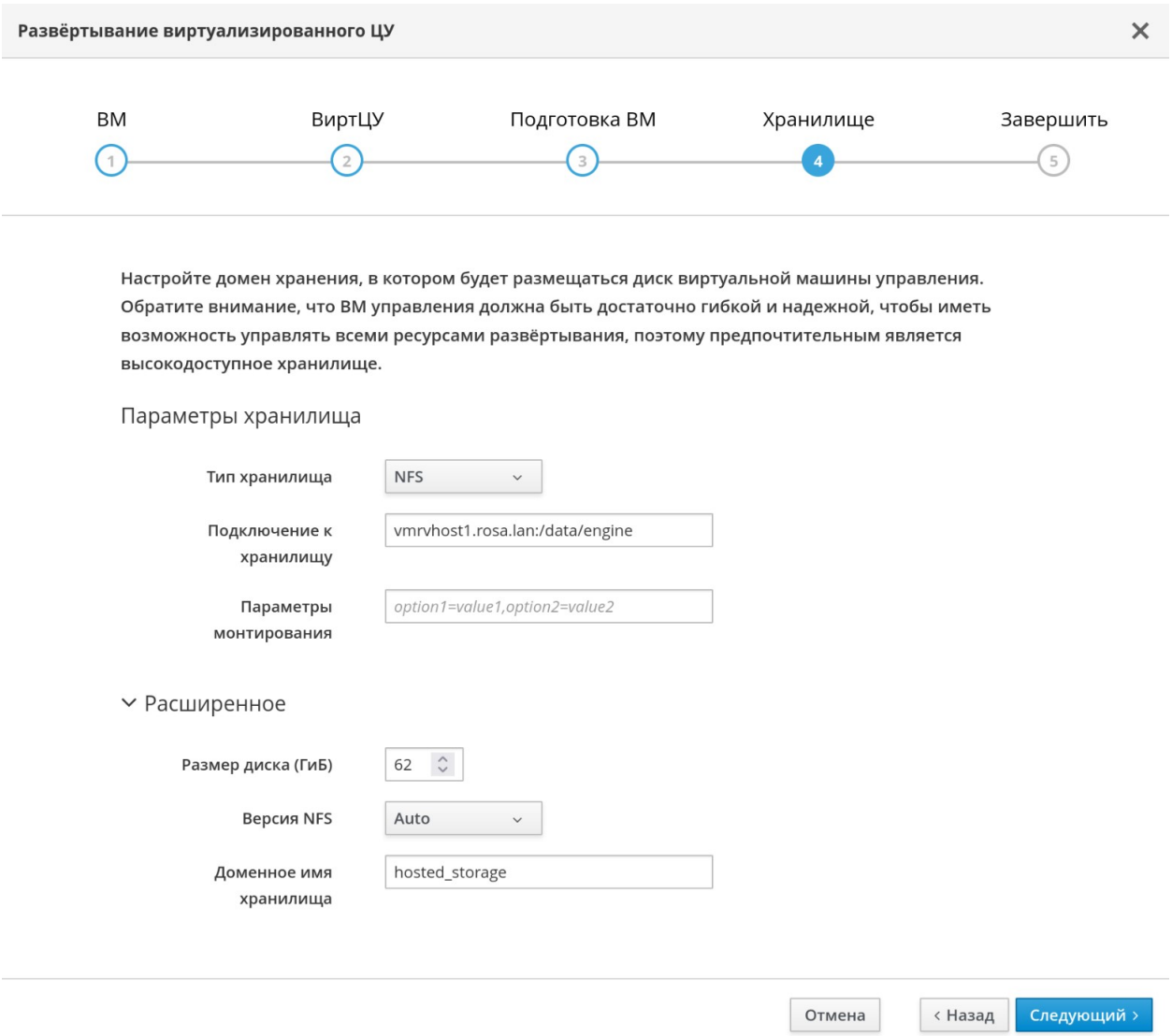

Рисунок 50 – Настройка расширенных параметров для хранилища типа NFS

– Размер диска – Размер диска по умолчанию составляет **62 ГБ**. Такой размер диска является минимально допустимым значением. При необходимости размер диска можно увеличить. Меньший размер диска использовать нельзя.

– Версия NFS – Версия NFS по умолчанию – "Auto". Данный параметр менять не рекомендуется.

– Доменное имя хранилища – Имя хранилища, по которому оно будет видно в домене.

3.5.2.4.4 Настройка хранилища типа iSCSI

Настройте параметры хранилища типа iSCSI (рисунок 51):

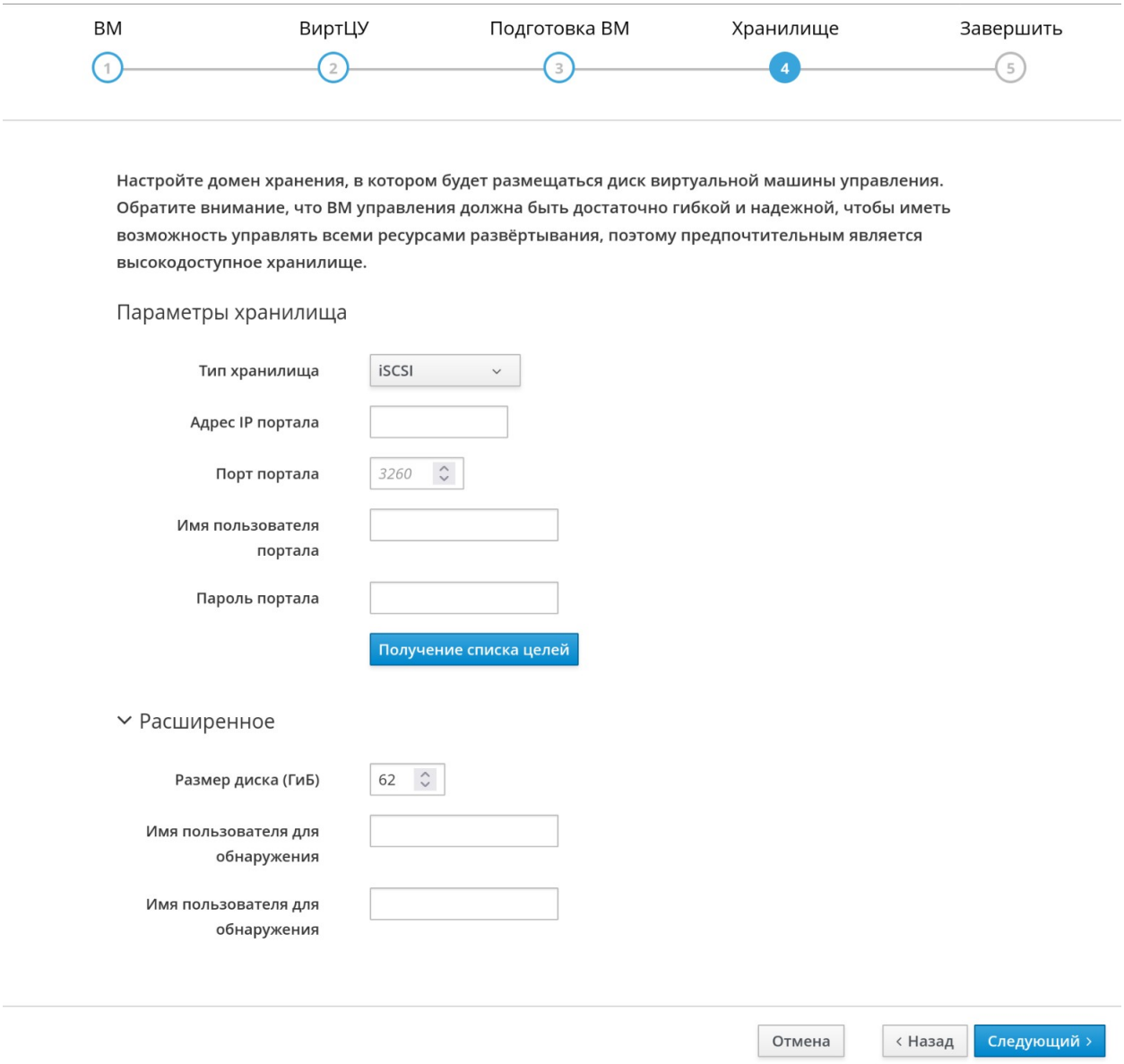

Рисунок 51 – Параметры хранилища типа iSCSI

– Адрес IP портала – IP-адрес, по которому доступен портал.

– Порт портала – Порт, по которому доступен портал (по умолчанию используется порт 3260).

– Имя пользователя портала – Имя пользователя портала, используемое для аутентификации.

– Пароль портала – Пароль пользователя портала.

Расширенные параметры для настроек хранилища типа iSCSI:

– Размер диска – Размер диска по умолчанию составляет **62 ГБ**. Такой размер диска является минимально допустимым значением. При необходимости размер диска можно увеличить. Меньший размер диска использовать нельзя.

– Имя пользователя обнаружения – Имя, по которому пользователь может быть обнаружен.

– Пароль пользователя обнаружения – Пароль пользователя.

Примечание – С особенностями настроек параметров хранилища iSCSI можно ознакомиться на сайте http://www.open-iscsi.com/.

При выборе типа хранилища iSCSI нажмите кнопку Получение списка целей для настройки параметров хранилища.

Нажмите кнопку Следующий для перехода к секции "Завершить".

3.5.2.4.5 Подключение хранилища типа Ceph

Отказоустойчивое хранилище CephFS может быть подключено как домен хранения к Платформе виртуализации ROSA Virtualization. Предварительно должна быть развернута базовая конфигурация ROSA Virtualization, предназначенная для использования в промышленном режиме функционирования с использованием хранилища типа NFS, Gluster или iSCSI.

Процедура подключения хранилища CepFS подробно описана в документе "ROSA Virtualization v3.1. Руководство по установке. Подключение отказоустойчивого хранилища CephFS".

3.5.2.4.5.1 Требования к программным и аппаратным средствам для подключения хранилища CephFS

Платформа виртуализации ROSA Virtualization:

– Развернута базовая конфигурация ROSA Virtualization, предназначенная для использования в промышленном режиме функционирования в качестве платформы виртуализации вычислительных центров.

– Используется версия ROSA Virtualization 3.1 или новее.

Отказоустойчивое хранилище Ceph:

– Развернута конфигурация отказоустойчивого хранилища Ceph – кластер, хосты, мониторы (MON), серверы метаданных (MDS), устройства хранения объектов (OSD).

– Используется версия Ceph 18.x или 19.x.

3.5.2.5 Завершение развертывания виртуализированного ЦУ

В секции "Завершить" нажмите кнопку Завершить развертывание для переноса ВМ СУСВ в хранилище и завершения процедуры установки СУСВ (рисунок 52).

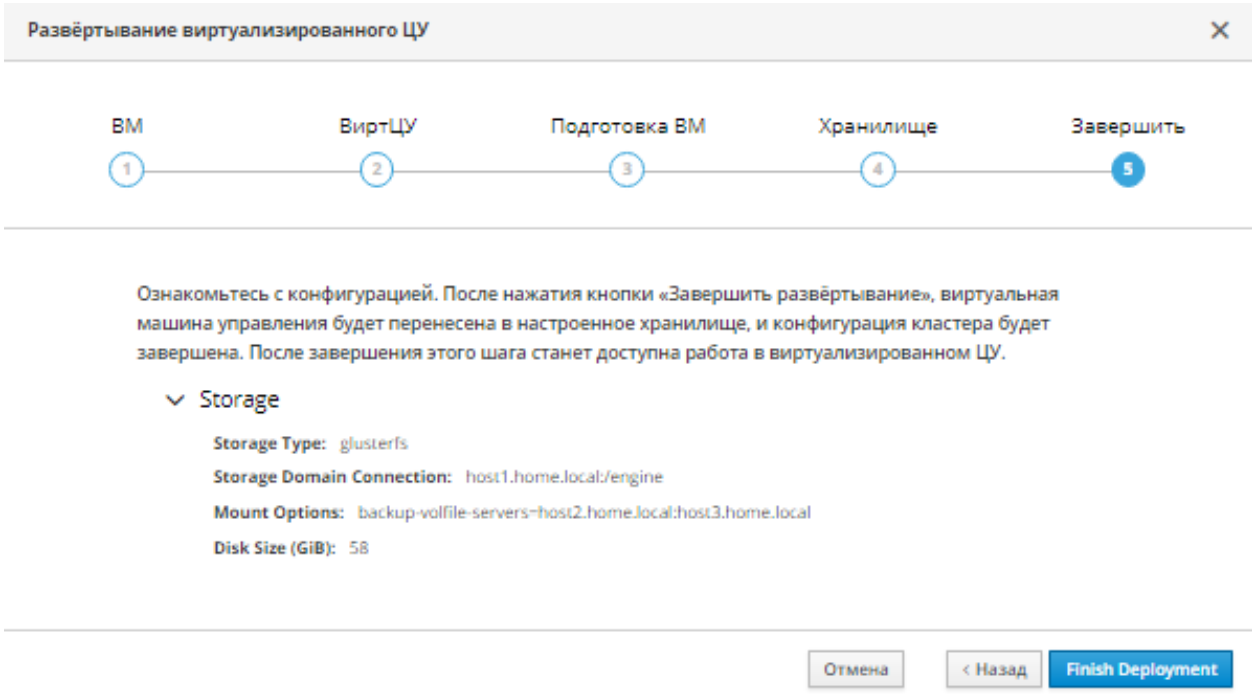

Рисунок 52 – Обзор конфигурации хранилища

После успешного завершения установки СУСВ на экране появится соответствующее сообщение и станет доступным вход в веб-интерфейс СУСВ (рисунок 53).

Рисунок 53 – Завершение установки СУСВ

Нажмите кнопку Закрыть для завершения работы программы установки СУСВ.

3.5.3 Очистка параметров установки СУСВ

В случае неудачного завершения установки СУСВ осуществите процедуру очистки данных перед повторной установкой. Для этого в консоли хоста дважды выполните следующую команду:

```
# ovirt-hosted-engine-cleanup
```

3.5.4 Установка СУСВ в консольном режиме

При необходимости установку СУСВ можно осуществить в консольном режиме. Для запуска программы установки выполните в консоли хоста следующую команду:

```
# hosted-engine --deploy
```

Далее следуйте инструкциям текстового интерфейса программы установки.

3.5.5 Установка сертификата ЦС

При первом доступе к Порталу администрирования (СУСВ) необходимо установить сертификат, используемый виртуализированным ЦУ, во избежание предупреждений безопасности.

3.5.5.1 Установка сертификата ЦС с использованием веб-браузера Firefox

Для установки сертификата ЦС с использованием веб-браузера Firefox:

1) Перейдите по адресу URL Портала администрирования и на странице приветствия нажмите на ссылку "CA сертификат центра управления" (рисунок 54).

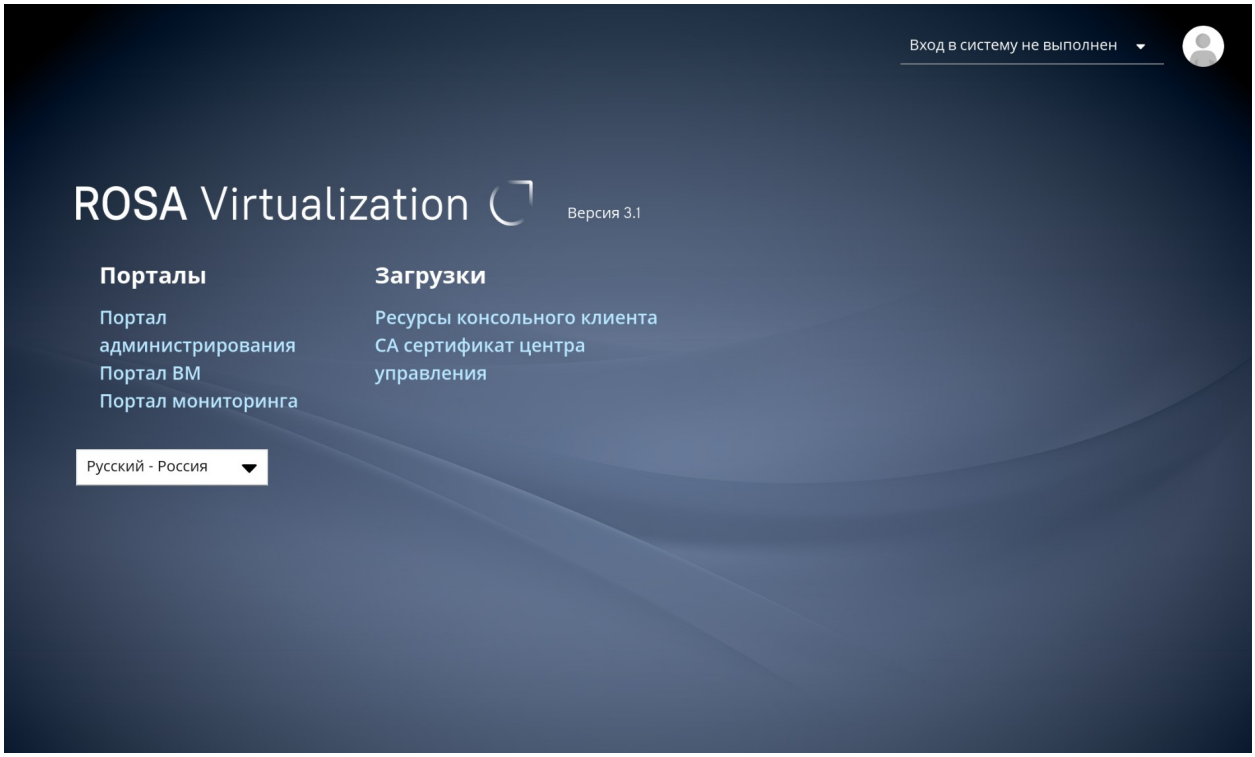

Рисунок 54 – Портал входа ROSA Virtualization: Портал администрирования, Портал ВМ

2) Будет загружен файл pki-resource (без расширения файла).

3) Откройте окно "Параметры/Предпочтения":

– Windows: откройте меню Firefox и выберите "Настройки" (URL about:preferences);

– Mac: откройте меню Firefox и выберите "Параметры...";

– Linux: откройте меню Правка и выберите "Параметры";

4) Выберите в меня слева раздел "Приватность и защита" и прокрутите вниз содержимое формы до секции "Сертификаты" (рисунок 55).

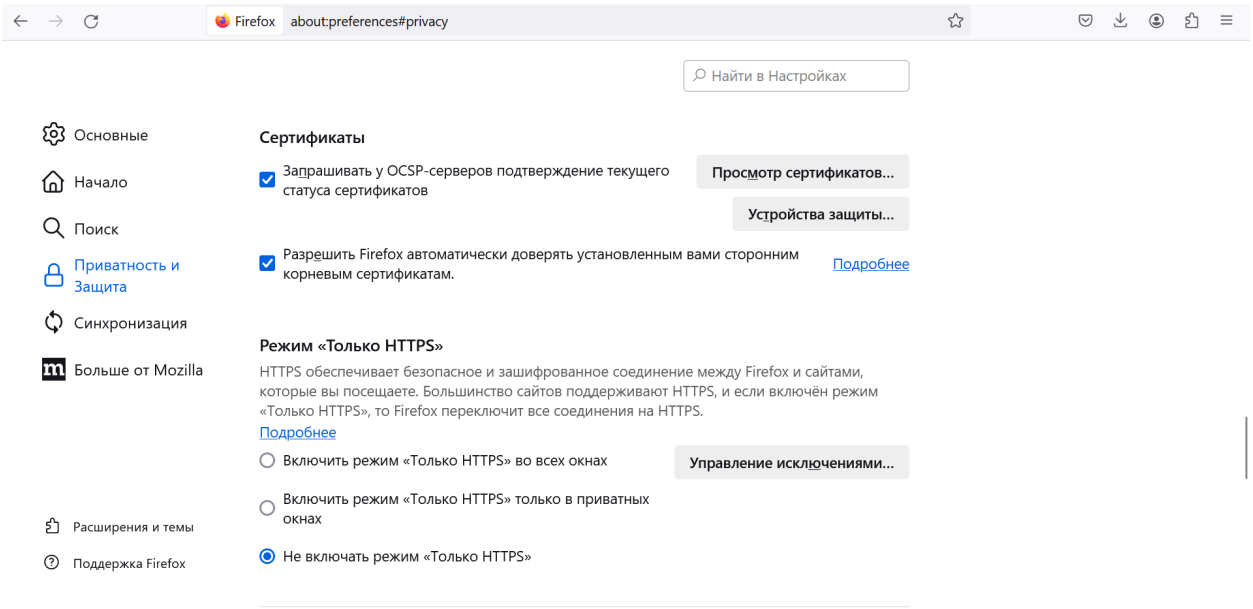

Рисунок 55 – Firefox: Раздел "Приватность и защита", секция "Сертификаты"

5) Нажмите Просмотр сертификатов…, чтобы открыть "Управление сертификатами" и перейти на вкладку "Центры сертификации" (рисунок 56).

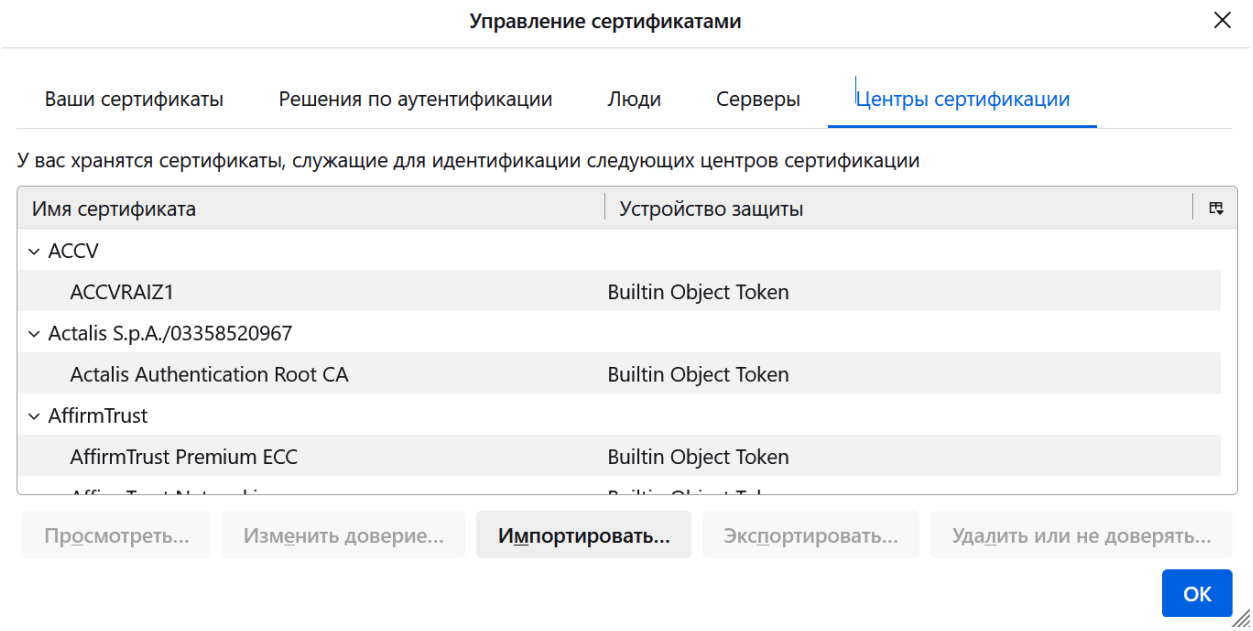

Рисунок 56 – Firefox: "Управление сертификатами" – вкладка "Центры сертификации"

6) Нажмите на кнопку Импортировать… (рисунок 56)

7) Выберите файл корневого сертификата, который нужно импортировать (для просмотра загруженного файла смените тип файла на "Все файлы").

8) Отметьте галочками параметры доверия и нажмите кнопку `OK`.

9) В разделе Диспетчера сертификатов нажмите кнопку `OK` и закройте окно "Параметры/Предпочтения".

10) Убедитесь в том, что все процессы Firefox остановлены.

11) Перезапустите Firefox и перейдите по адресу URL Портала администрирования. Значок замочка в адресной строке указывает на то, что сертификат ЦС установлен.

3.5.5.2 Установка сертификата ЦС в веб-браузере Google Chrome

Для установки сертификата ЦС в веб-браузере Google Chrome:

1) Перейдите по адресу URL Портала ВМ и на странице приветствия нажмите на кнопку `CA сертификат центра управления` (рисунок 57).

2) Будет загружен файл pki-resource.cer (расширение файла .cer).

3) Перейдите в меню "Настройки → Конфиденциальность и безопасность → Настроить сертификаты" (рисунок 57) и нажмите на значок (квадрат со стрелочкой) для вызова диалога управления сертификатами (URL chrome://settings/security).

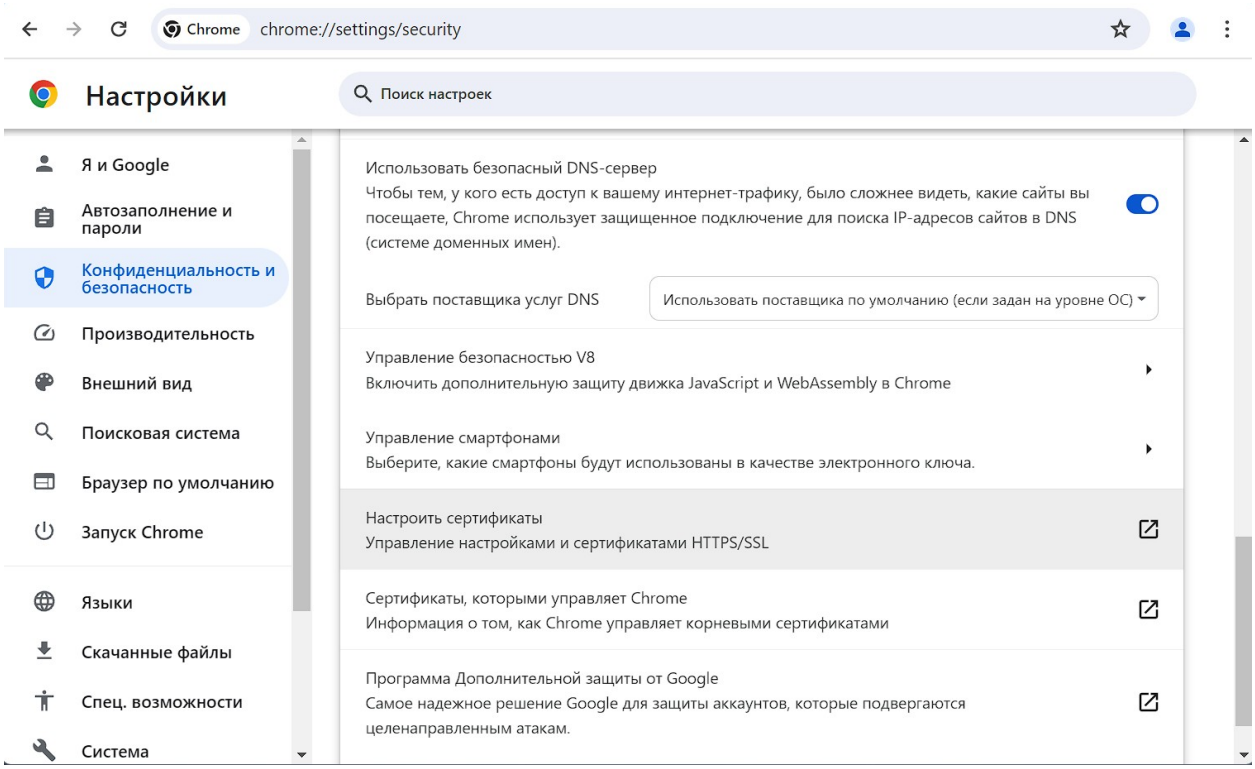

Рисунок 57 – Chrome: Настройки → Конфиденциальность и безопасность → Настроить сертификаты

4) В диалоге управления сертификатами нажмите кнопку Импорт… (рисунок 58).

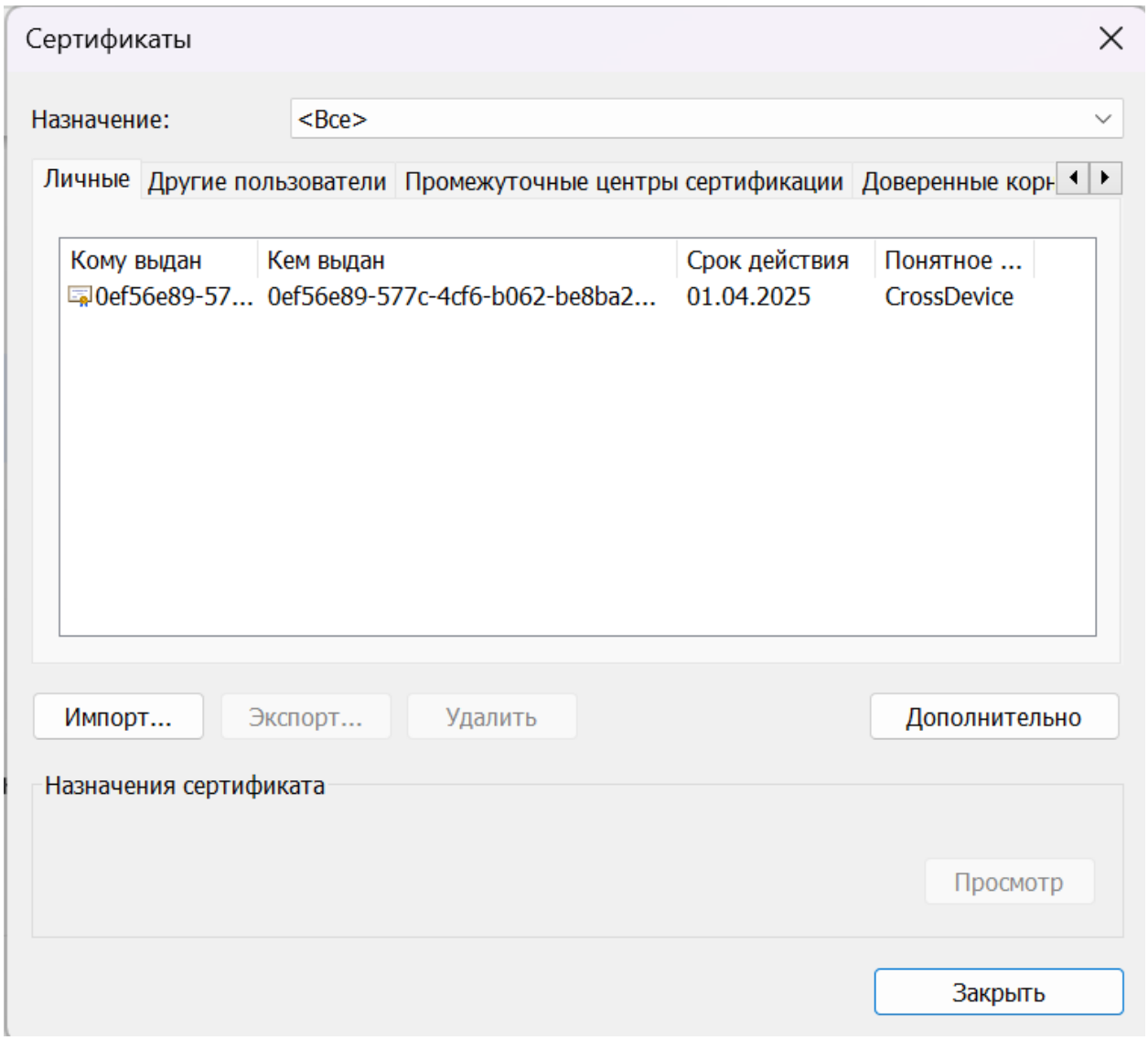

Рисунок 58 – Chrome: диалог для управления сертификатами

Откроется окно "Мастер импорта сертификатов" (рисунок 59).

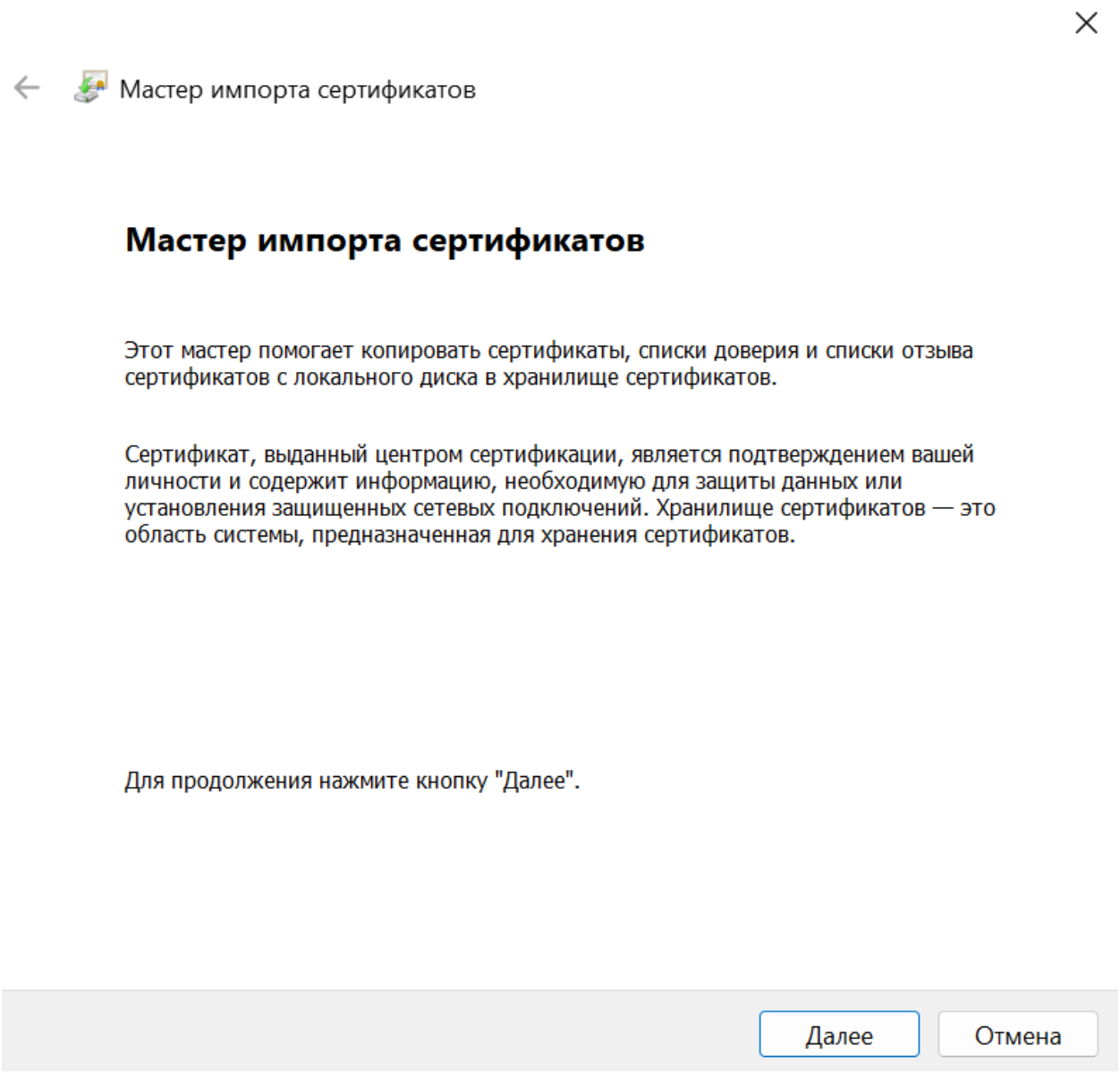

Рисунок 59 – Мастер импорта сертификатов (Windows)

Нажмите кнопку Далее.

5) В "Мастере импорта сертификатов" укажите "Импортируемый файл", для чего нажмите на кнопку Обзор… (рисунок 60).

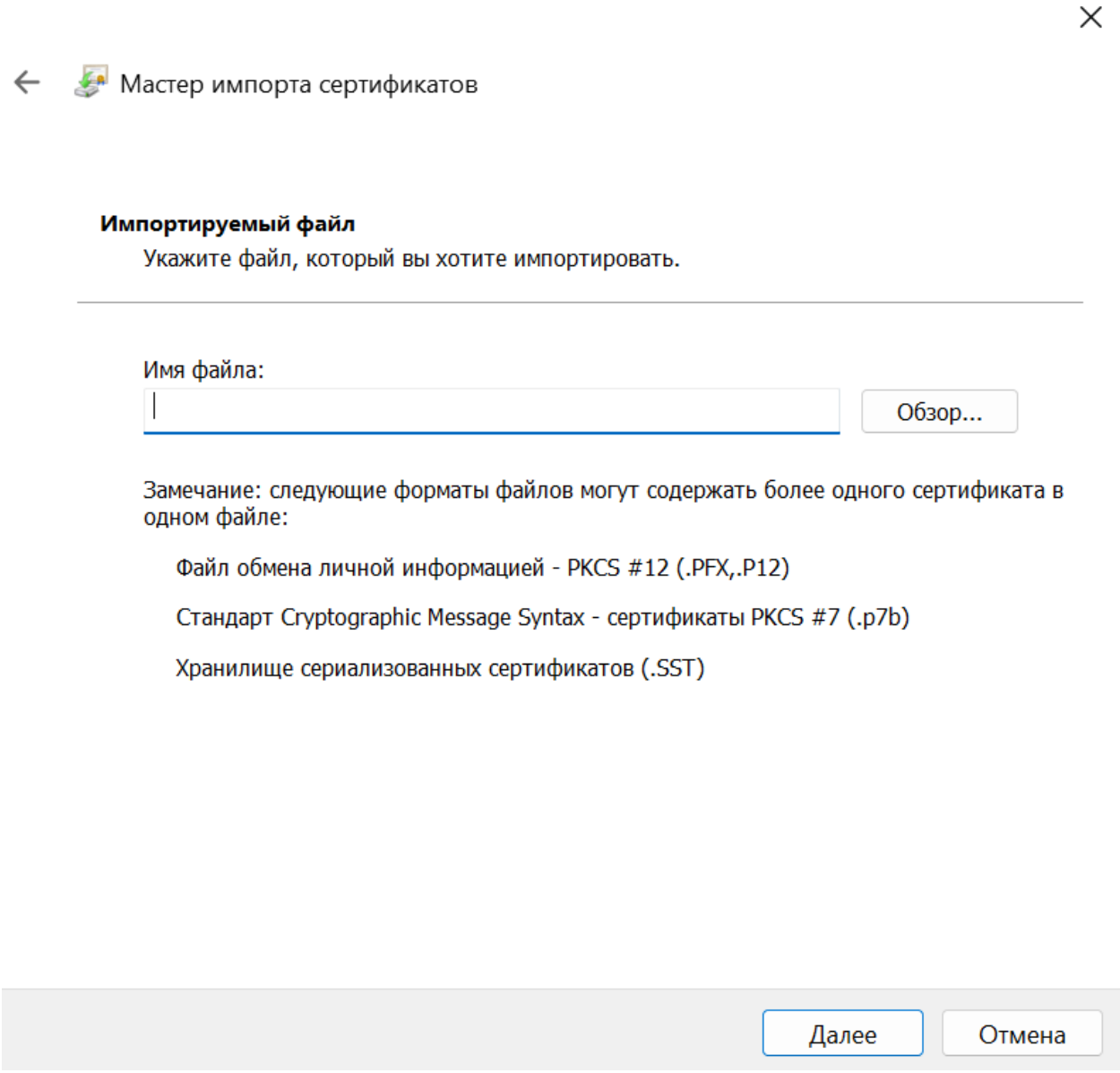

Рисунок 60 – Мастер импорта сертификатов – выбор Импортируемый файл

6) Выберите файл корневого сертификата X.509, который нужно импортировать (рисунок 61). Для просмотра всех файлов смените тип файла на "Все файлы"; необходим ранее загруженный файл pki-resource.cer.

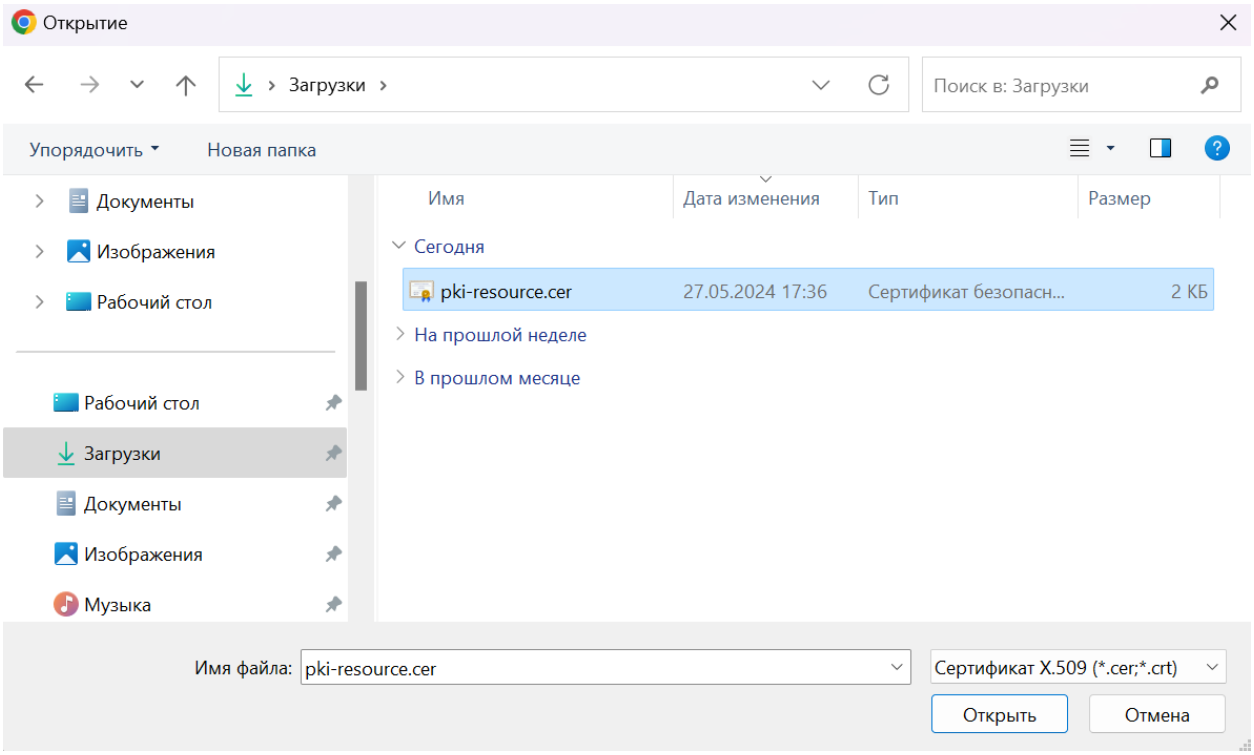

Рисунок 61 – Выбор файла корневого сертификата X.509 (Windows)

7) В "Мастере импорта сертификатов" укажите необходимое "Хранилище сертификатов" из "Доверенных корневых центров сертификации" (рисунок 62) и нажмите на кнопку Далее.

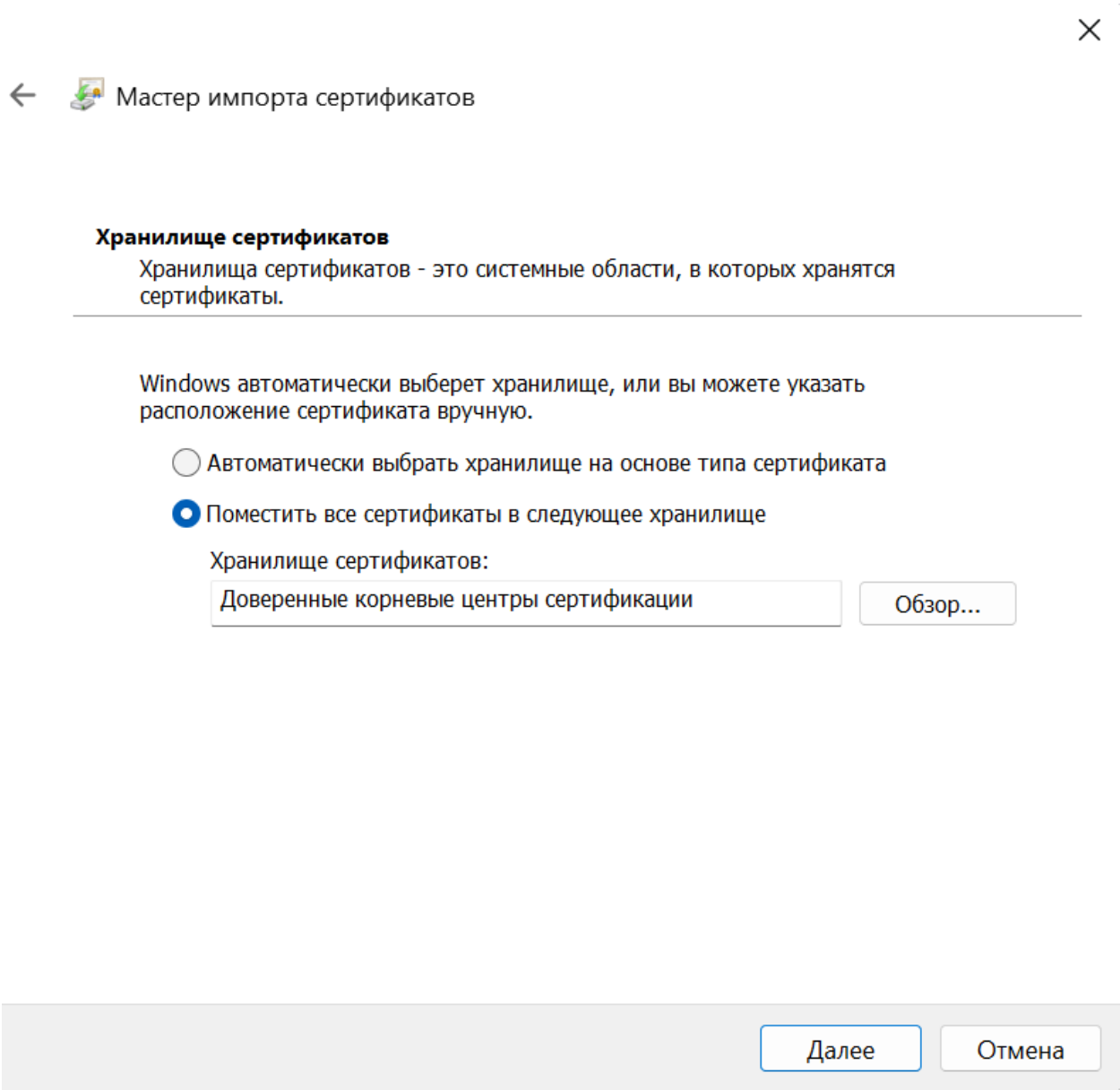

Рисунок 62 – Мастер импорта сертификатов: Хранилище сертификатов – Доверенные корневые центры сертификации

8) В завершающем диалоге "Мастера импорта сертификатов" нажмите на кнопку Готово (рисунок 63).

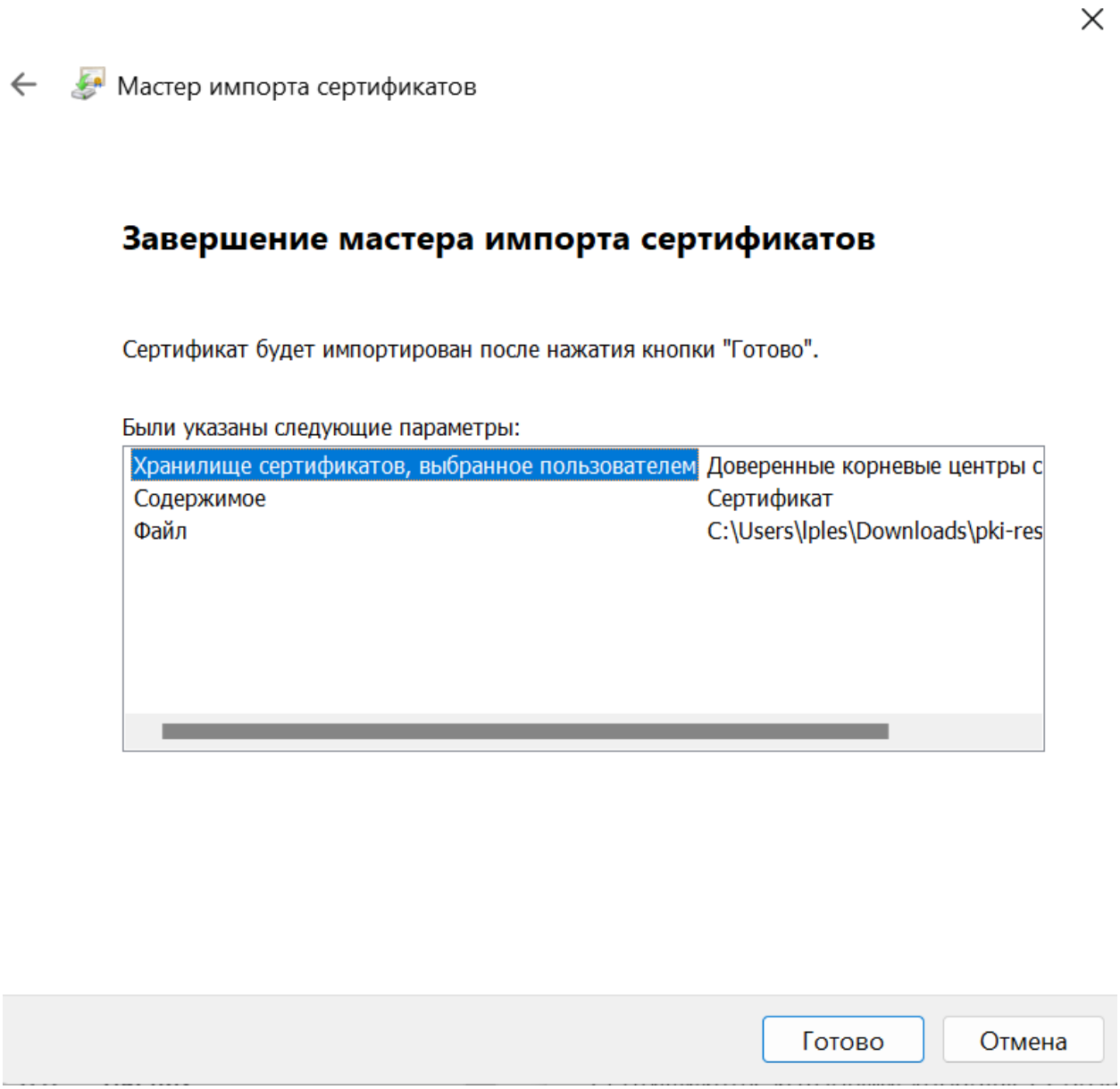

Рисунок 63 – Завершающий диалог "Мастера импорта сертификатов"

9) Закройте Chrome и убедитесь в том, что все процессы Chrome остановлены.

10) Перезапустите Chrome и перейдите по адресу URL Портала администрирования (СУСВ). Значок замочка в адресной строке указывает на то, что сертификат ЦС установлен (рисунок 64).

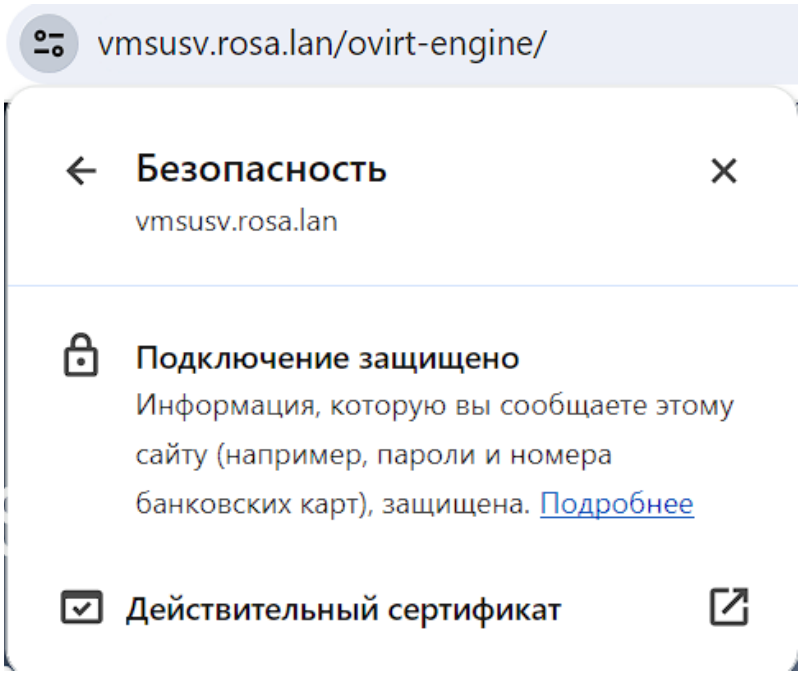

Рисунок 64 – Подключение к СУСВ (Портал администрирования) защищено

3.5.6 Вход в веб-интерфейс СУСВ

Для доступа к веб-интерфейсу введите в адресной строке браузера (на внешней рабочей станции) доменное имя или IP-адрес ВМ СУСВ, например:

```
https://susv.rosa.lan
```

На экране появится окно, содержащее ссылки для перехода к "Порталу администрирования" или "Порталу ВМ" (рисунок 65).

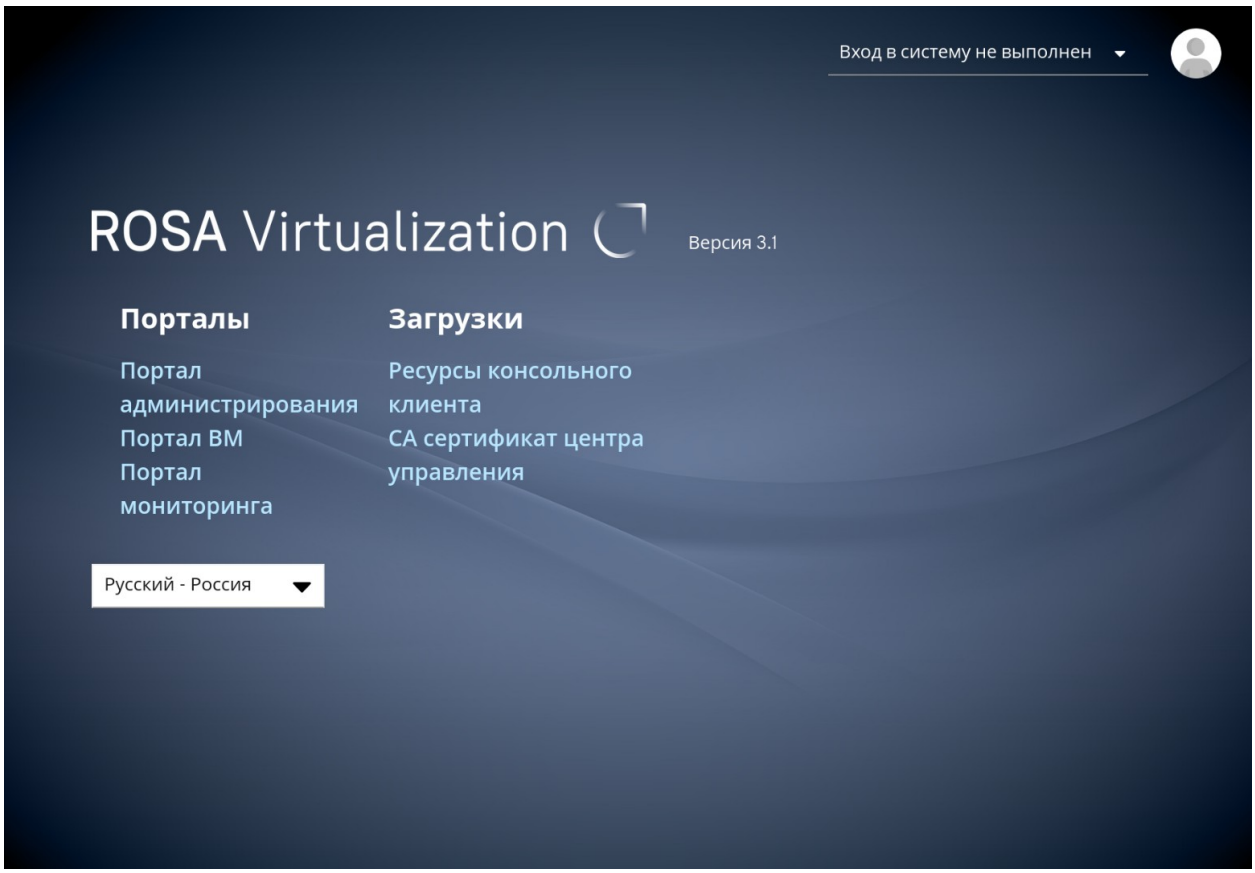

Рисунок 65 – Интерфейс выбора портала: Портал администрирования, Портал ВМ

Для доступа к административным функциям СУСВ нажмите на ссылку "Портал администрирования" и введите учетные данные (логин и пароль) пользователя admin, профиль "Internal" для авторизации (рисунок 66).

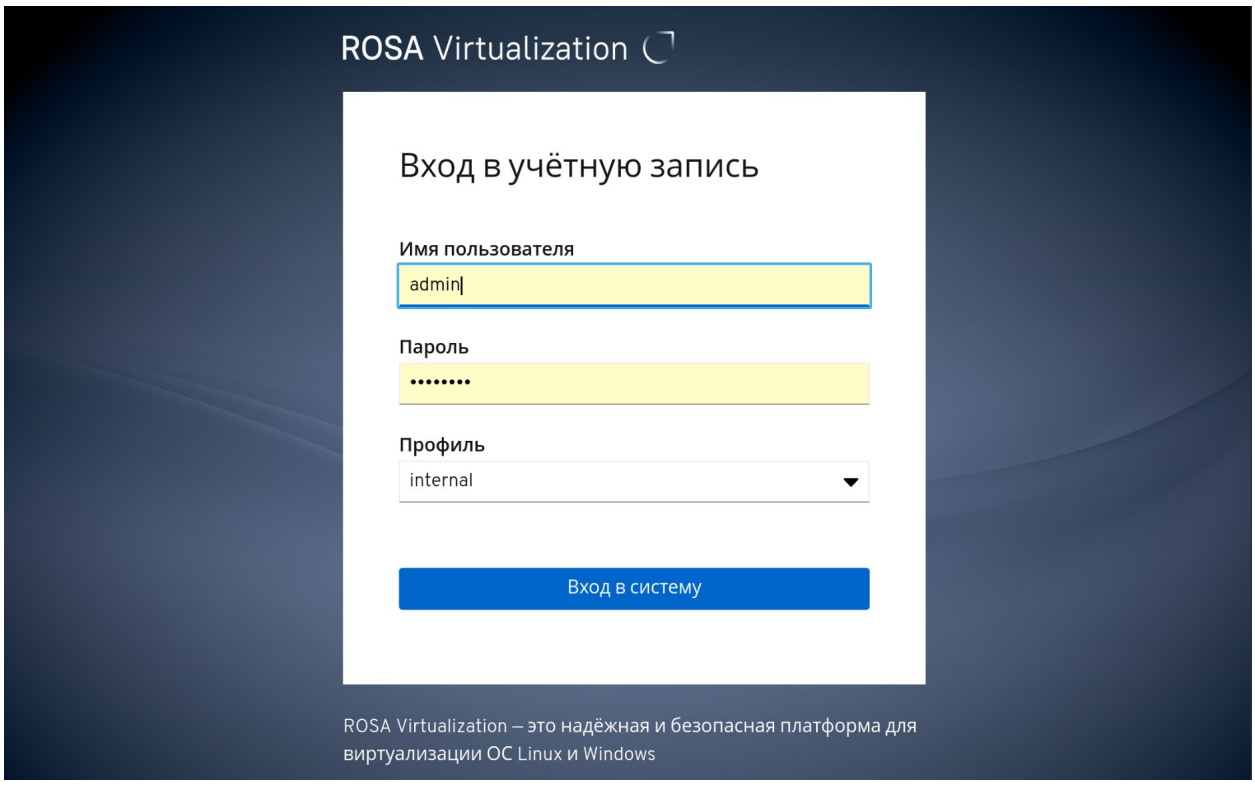

Рисунок 66 – Вход в учётную запись ROSA Virtualization

В случае успешной авторизации на экране появится панель мониторинга СУСВ, которая загружается по умолчанию и содержит общую информацию о компонентах ROSA Virtualization (рисунок 67).

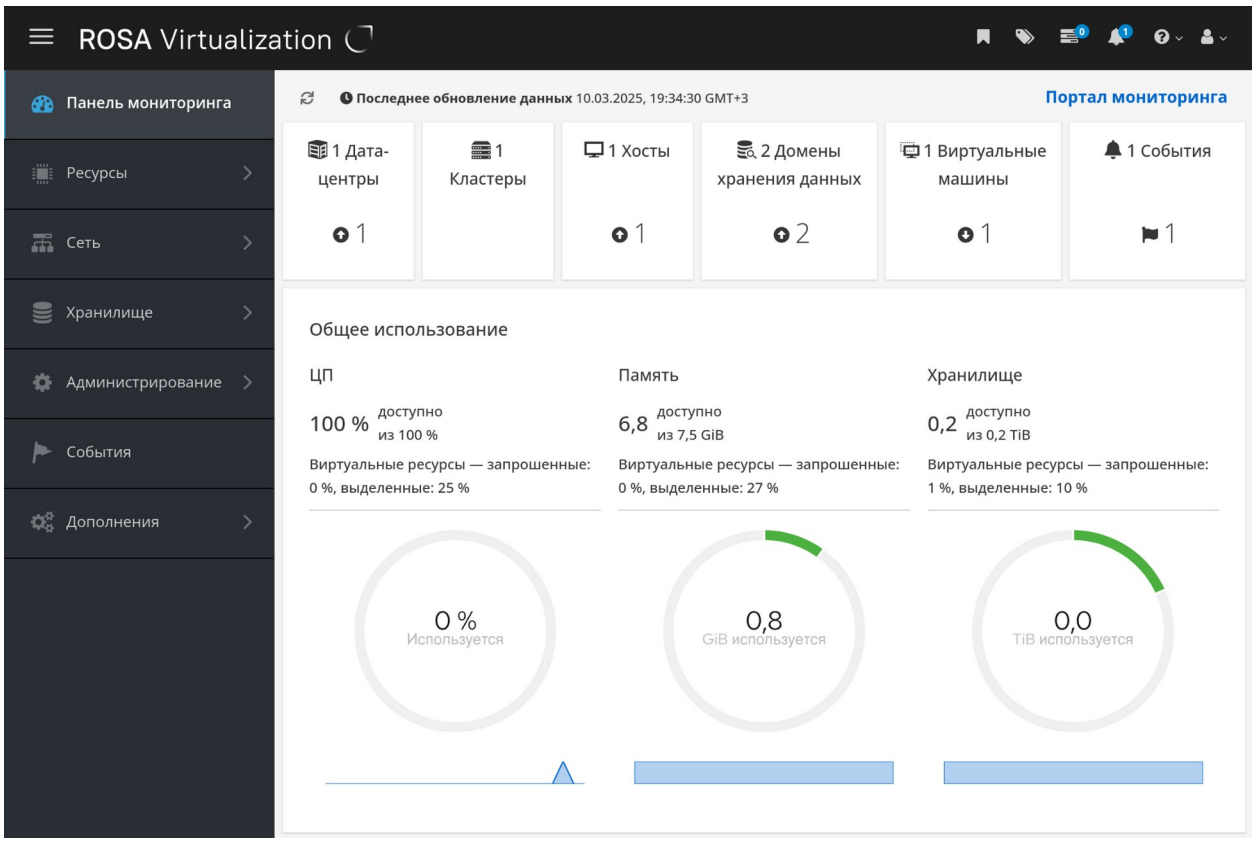

Рисунок 67 – Панель мониторинга СУСВ

Последующий доступ к функциям СУСВ осуществляется через выбор необходимых пунктов в главном меню СУСВ (рисунок 68).

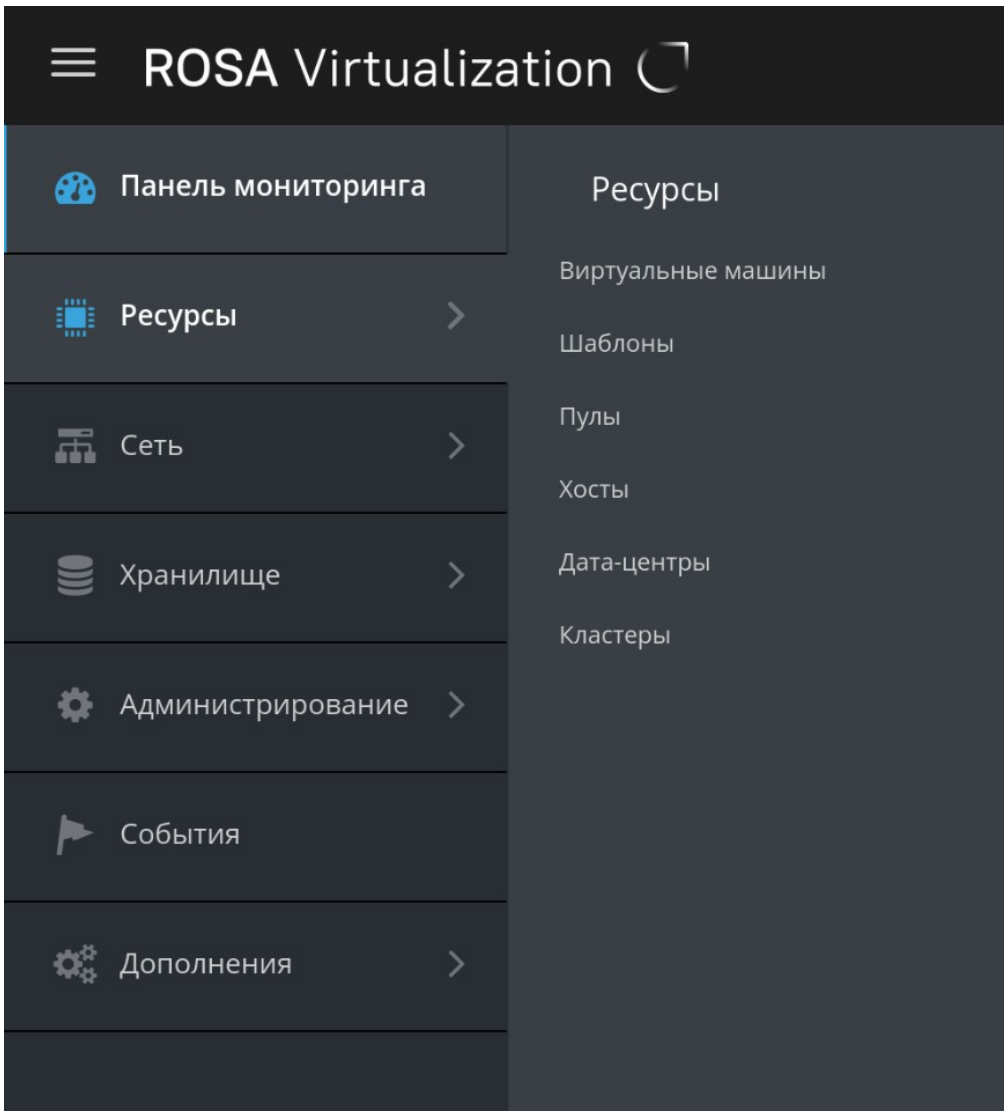

Рисунок 68 – Главное меню веб-интерфейса СУСВ, с открытым подменю "Ресурсы"

3.6 Добавление хостов в кластер

При развертывании ROSA Virtualization в базовой конфигурации выполните процедуру добавления **каждого из хостов** с установленным гипервизором в кластер.

Кластер – логическое объединение хостов, которые выступают в качестве общего ресурсного пула для ВМ. При этом ВМ динамически выделяются каждому хосту в кластере и могут мигрировать между хостами.

Каждый хост ROSA Virtualization должен принадлежать определенному кластеру.

Во время установки ROSA Virtualization создается кластер по умолчанию Default, который включает в свой состав только хост с установленным гипервизором и развернутой ВМ СУСВ (например, "rvhost1.rosa.lan").

3.6.1 Добавление хостов в кластер с использованием портала администрирования СУСВ

Добавление хостов в кластер осуществляется на портале администрирования СУСВ.

Для добавления хоста выберите пункт "Ресурсы → Хосты" в главном меню СУСВ и нажмите кнопку Добавить.

На экране появится вкладка "Общее" окна "Новый хост" (рисунок 69).

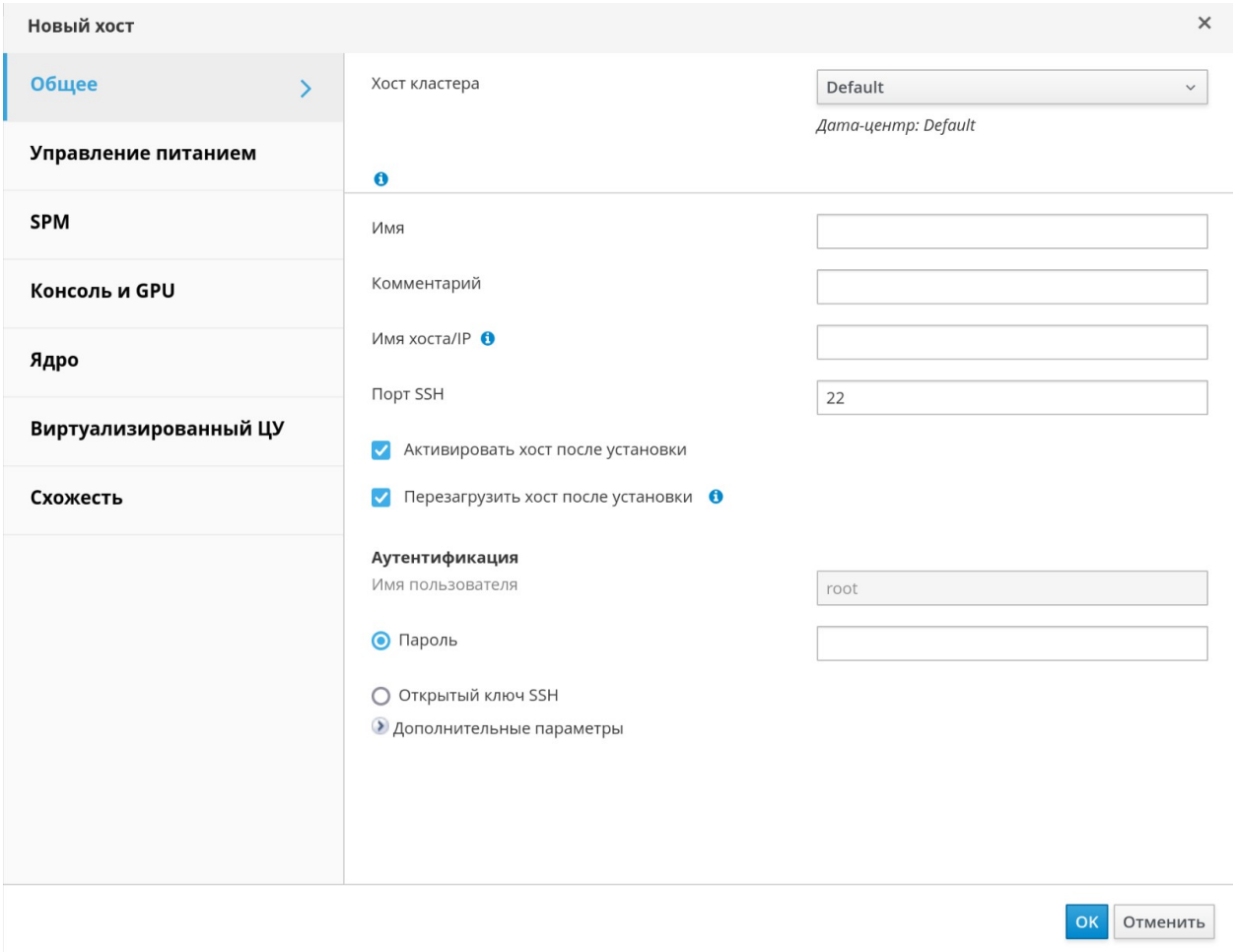

Рисунок 69 – Вкладка "Общее" окна "Новый хост"

В поля "Имя" и "Имя хоста/IP" введите соответственно краткое (например, "rvhost2") и полное доменное имя хоста (например, "rvhost2.rosa.lan") или его IP-адрес.

В поле "Пароль" укажите пароль учетной записи суперпользователя root данного хоста.

Далее перейдите на вкладку "Виртуализированный ЦУ" и выберите действие "Развернуть", чтобы данный хост имел возможность запуска СУСВ при выходе из строя хоста, на котором СУСВ выполняется в текущий момент, что повышает надежность и отказоустойчивость ROSA Virtualization.

Для применения всех сделанных изменений нажмите кнопку OK.

Для настройки политики энергосбережения на экране появится окно "Параметры управления питанием". При необходимости в настройке параметров агента интерфейса низкоуровнего управления питанием хоста нажмите кнопку Настроить управление питанием и введите необходимые параметры.

Для завершения процедуры добавления хоста в кластер нажмите кнопку ОК.

После добавления в кластер статус хоста изменится на значение "Up".

Повторите процедуру добавления в кластер для каждого из хостов с установленным гипервизором.

3.7 Активация лицензии ROSA Virtualization

Лицензия ROSA Virtualization предназначена для подтверждения уникальности копии программного продукта и устанавливает определенные ограничения по применению, такие как допустимое количество совместно работающих ВМ, задействованных процессорных слотов и т.д. Дополнительно лицензия имеет дату окончания действия, после наступления которой запуск ВМ будет заблокирован.

Файл с лицензией ROSA Virtualization содержит электронный ключ, который необходимо активировать на СУСВ. Лицензия может быть активирована двумя способами:

– Плагин в веб-интерфейсе Портала администрирования.
– Командная строка (терминал) СУСВ.

3.7.1 Активация лицензии в веб-интерфейсе Портала администрирования

Для активации лицензии ROSA Virtualization откройте меню "Дополнения" Портала администрирования и выберите секцию "Лицензирование".

Откроется окно для управления лицензированием ROSA Virtualization (рисунок 70).

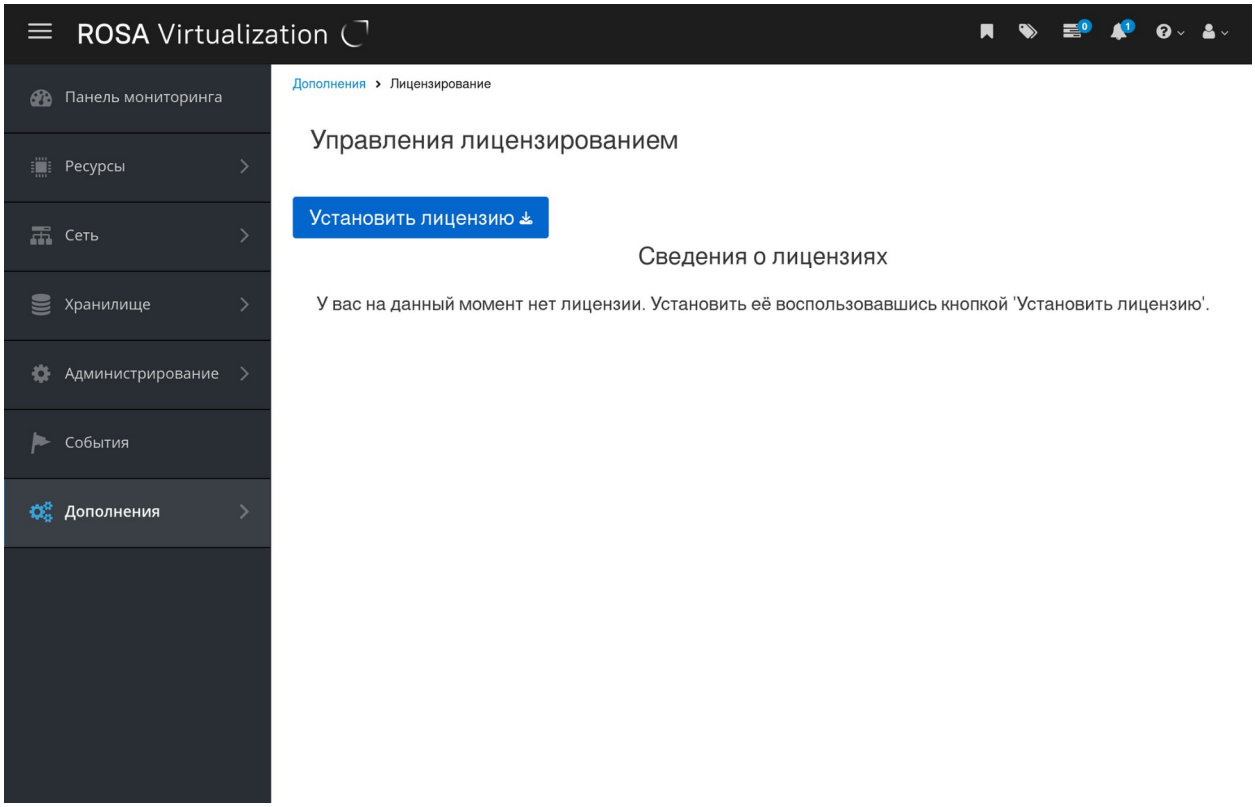

Рисунок 70 – Управление лицензированием ROSA Virtualization

Нажмите на кнопку Установить лицензию для начала процесса установки лицензии (рисунок 70).

На экране откроется форма для установки лицензии (рисунок 71).

Если у вас есть лицензия (электронный ключ активации) в виде текстового файла, вы можете скопировать его содержимое в буфер обмена и вставить в поле ввода справа (секция "Вставить лицензию"). Затем нажмите на кнопку Загрузить и после валидации лицензии – на кнопку Закрыть.

Если на экран выводится сообщение "Неправильная лицензия", то лицензия не была валидирована. Нажмите на кнопку Повторить для возврата на экран управления лицензированием.

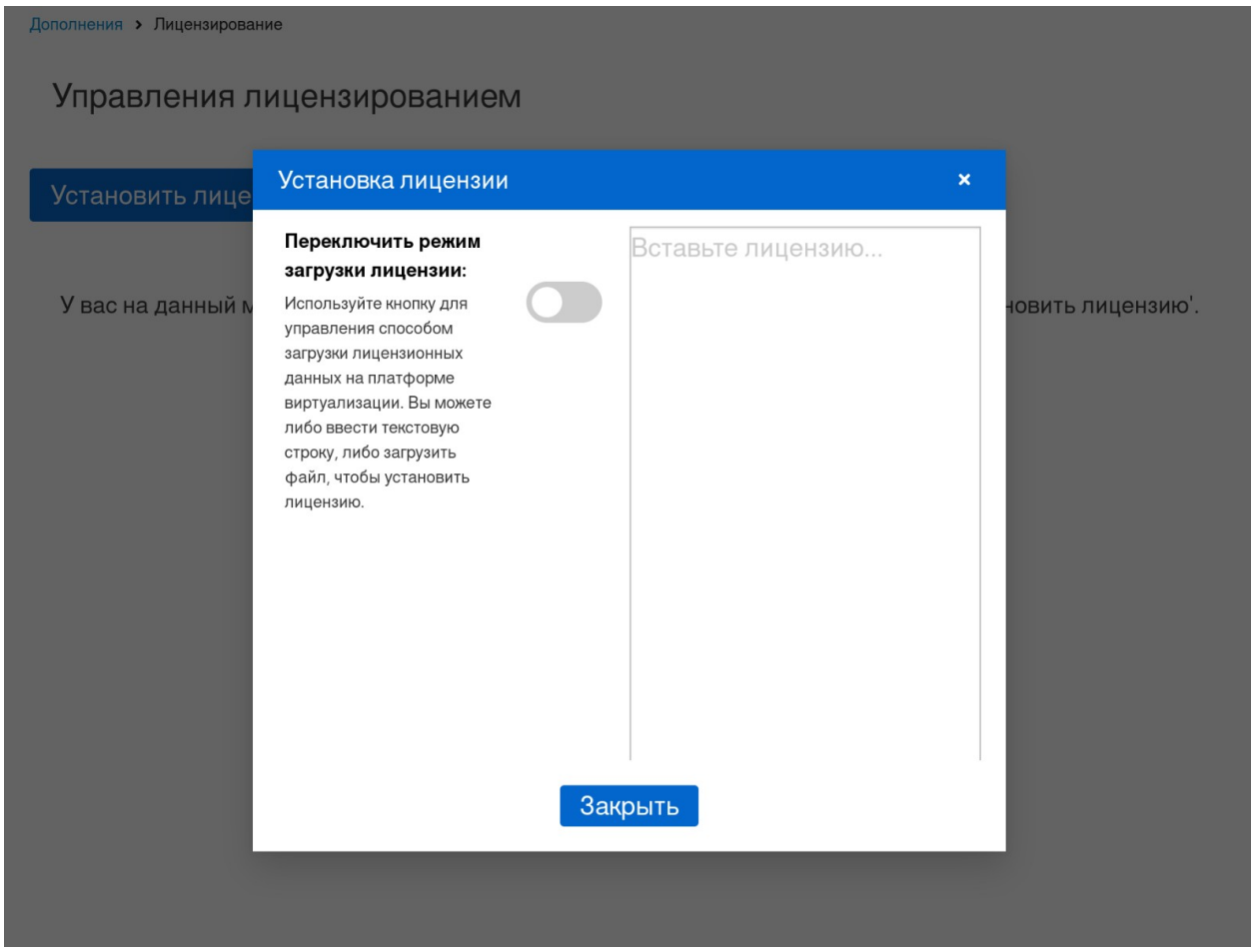

Рисунок 71 – Форма установки лицензии ROSA Virtualization

Если вы хотите загрузить лицензию (электронный ключ активации) через файл, то выполните следующие действия:

1) Используйте переключатель "Переключить режим загрузки лицензии" для изменения режима загрузки лицензии. При включении активируется режим загрузки файла. Также возможно перетащить файл в окно с помощью мыши (рисунок 72).

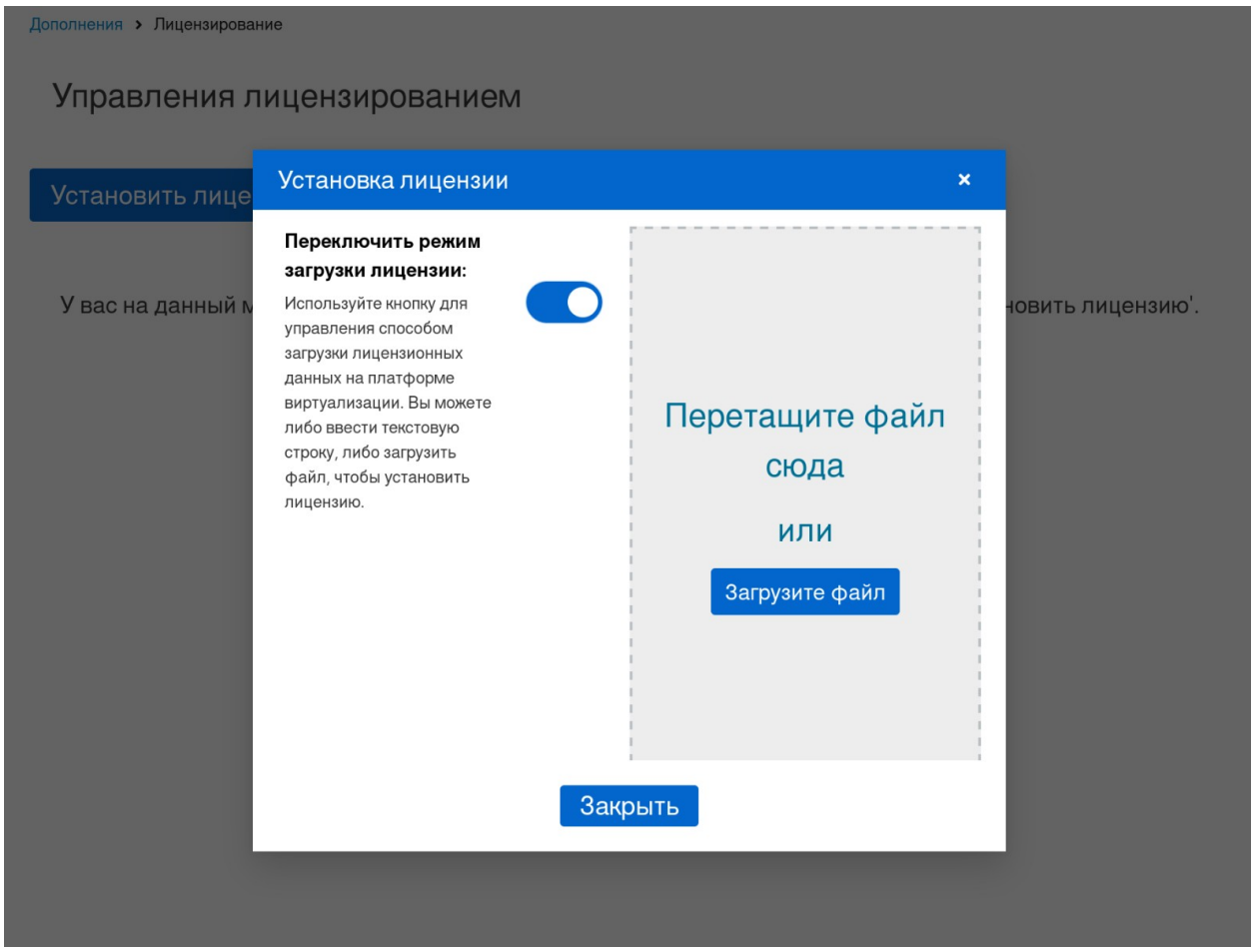

Рисунок 72 – Диалоговое окно загрузки файла лицензии

2) Перетащите файл с лицензией (в примере – license_rv.gz) в окно для загрузки или выберите файл с диска, используя файловый диалог (рисунок 73).

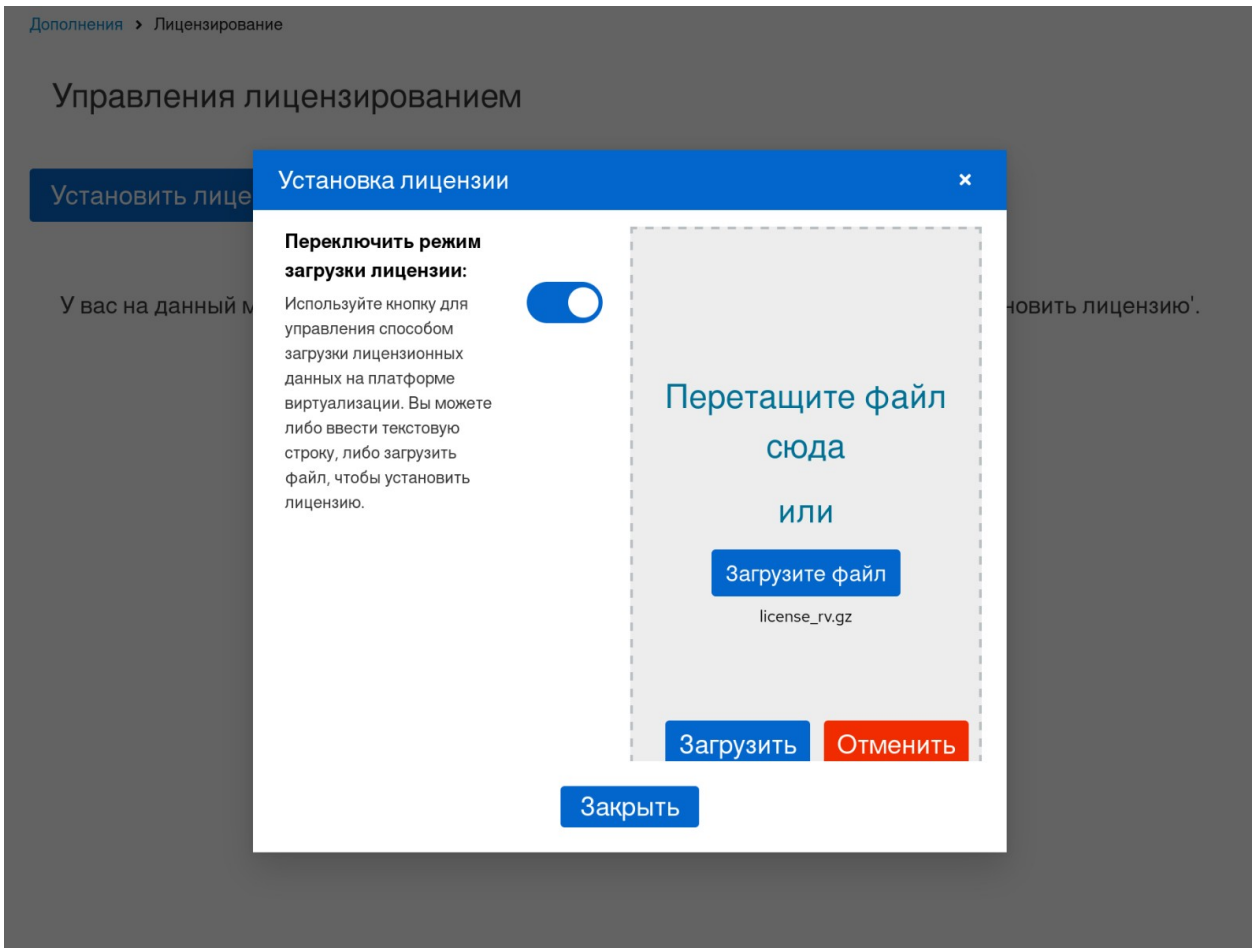

Рисунок 73 – Подтверждение загрузки лицензии

3) Нажмите на кнопку `Загрузить` для загрузки файла с лицензией или на кнопку `Отменить` – для отмены операции (рисунок 73).

На экране откроется окно с подтверждением загрузки лицензии (рисунок 74).

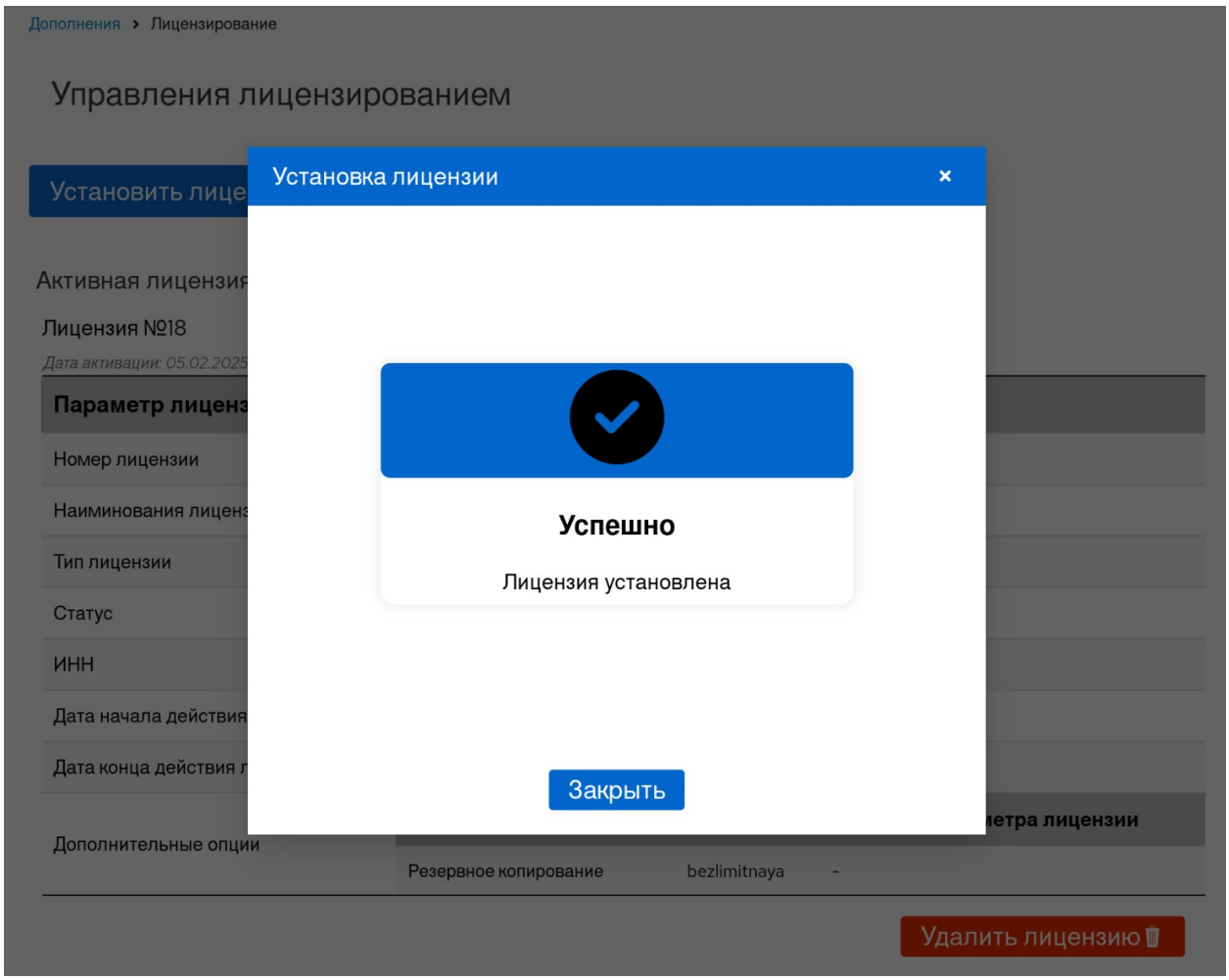

Рисунок 74 – Подтверждение успешности загрузки лицензии

4) Нажмите на кнопку Закрыть (рисунок 74).

Откроется окно управления лицензированием с информацией об установленной лицензии (рисунок 75).

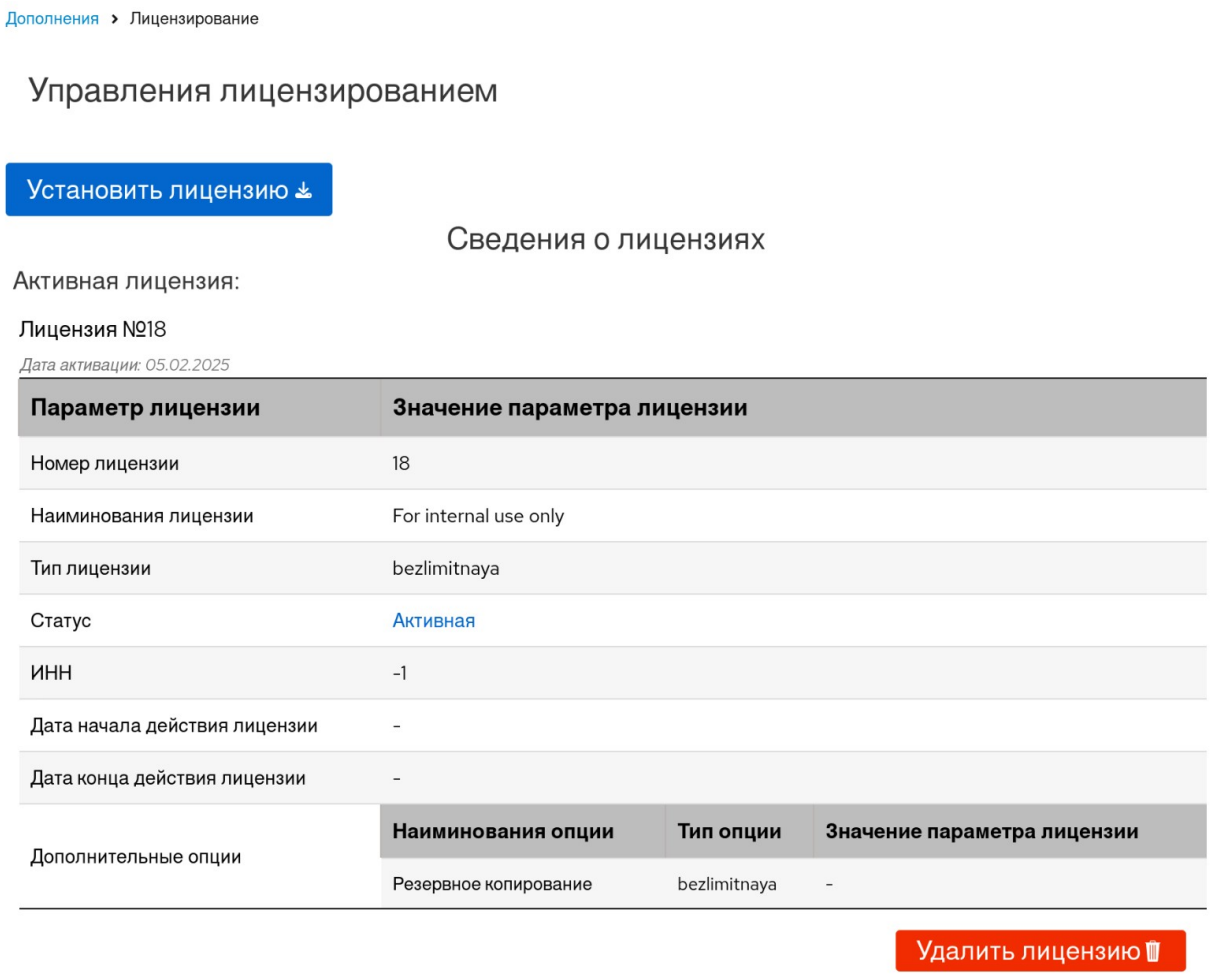

Рисунок 75 – Информация об установленной лицензии в веб-интерфейсе

При необходимости удаления лицензии и установки другой лицензии нажмите на кнопку `Удалить лицензию`.

3.7.2 Активация лицензии ROSA Virtualization через интерфейс CLI

Для активации лицензии ROSA Virtualization через интерфейс CLI:

1) Подключитесь к консоли СУСВ по SSH или откройте терминал в веб-интерфейсе администрирования хоста.

2) Скопируйте файл с лицензией ROSA Virtualization в один из каталогов ВМ СУСВ (например, `/tmp`). Для копирования можно использовать утилиту SCP (Secure Copy Protocol) или аналогичную ей.

Активация лицензии ROSA Virtualization осуществляется консольной утилитой `install-rosa-license`.

Примечание – Для подключения к консоли СУСВ по SSH выполните следующую команду с указанием доменного имени (например, "susv.rosa.lan") или IP-адреса ВМ СУСВ, а также пароля учетной записи суперпользователя root ВМ СУСВ при выводе на экран соответствующего запроса:

```
# ssh root@susv.rosa.lan
root@susv.rosa.lan"s password:
```

3) Для запуска процесса активации лицензии выполните в консоли СУСВ следующую команду:

```
# install-rosa-license
```

4) При выводе на экран соответствующего запроса введите путь к файлу с лицензией.

Далее интерактивный сценарий автоматически осуществит активацию лицензии ROSA Virtualization.

3.7.2.1 Пример активации лицензии ROSA Virtualization

Сценарий активации лицензии по умолчанию предполагает наличие файла с лицензией под именем license.gz в каталоге /tmp. Если вы скопировали файл с лицензией в это каталог, то достаточно нажать на клавишу `Enter`.

```
[root@susv ~]# install-rosa-license
Path to Rosa Virtualization license file (/tmp/license.gz):
The license is successfully installed.
```

Если в консоль было выведено сообщение "The license is successfully installed", то лицензия была успешно активирована.

Примечание – Для просмотра подробной информации и проверки валидности установленной лицензии выполните в консоли СУСВ следующую команду:

```
# rosa-license-info
```

3.7.2.2 Пример просмотра информации об лицензии

```
[root@susv ~]# rosa-license-info
VM_Backup appliance is allowed: 1.
ROSA license is valid.
```

Лицензия верифицирована. Для операций резервного копирования можно использовать один клиент (Backup Appliance).

3.8 Установка сервера IPA

В составе ROSA Virtualization сервер IPA функционирует в качестве сервера каталогов LDAP и предназначен для идентификации и аутентификации доменных пользователей.

Сервер IPA может быть развернут как на отдельном физическом сервере без предустановленной ОС, так и на ВМ под управлением ROSA Virtualization.

Для установки сервера IPA на ВМ под управлением ROSA Virtualization предварительно создайте новую ВМ на портале администрирования СУСВ, а также загрузите образ с дистрибутивом (файл RV-3.1-20250224.0-rv-x86_64-dvd1.iso) в хранилище в подкаталог /iso.

Для установки сервера IPA на отдельный физический сервер используйте DVD-диск с дистрибутивом ROSA Virtualization или ранее созданный сменный носитель с записанным на него образом дистрибутива.

3.8.1 Создание ВМ для сервера IPA

Для создания новой ВМ для сервера IPA авторизуйтесь на Портале администрирования СУСВ. На экране появится интерфейс Портала администрирования с главным меню СУСВ.

В главном меню СУСВ выберите пункт "Ресурсы → Виртуальные машины" и нажмите кнопку Добавить.

На экране появится вкладка "Общие" окна "Новая ВМ" (рисунок 76).

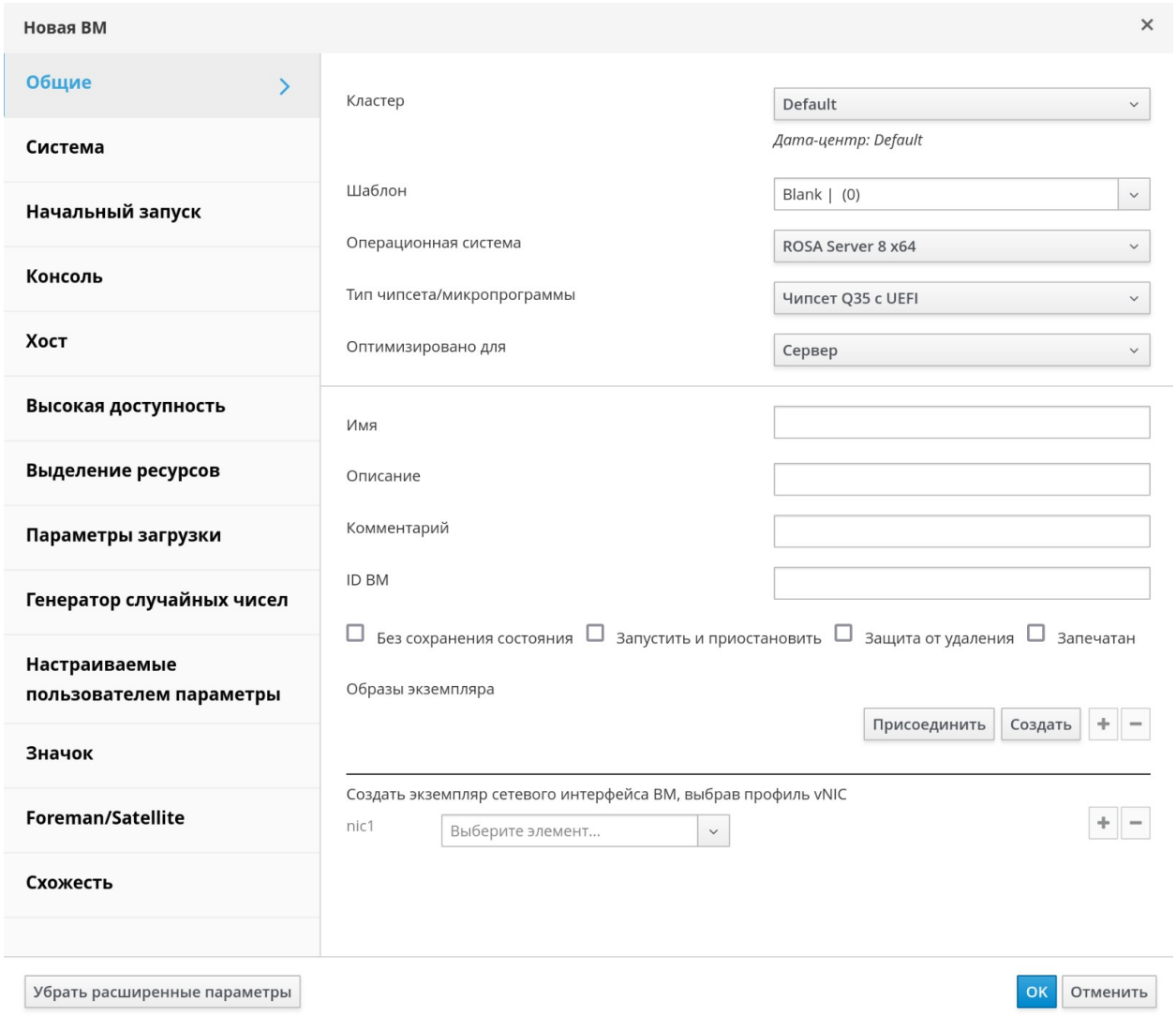

Рисунок 76 – Вкладка "Общие" окна "Новая ВМ"для создания новой виртуальной машины

В поле "Имя" введите уникальное наименование для новой ВМ (например, "Server-IPA").

Для создания виртуального диска ВМ нажмите кнопку Создать. На экране появится окно "Новый виртуальный диск" (рисунок 77).

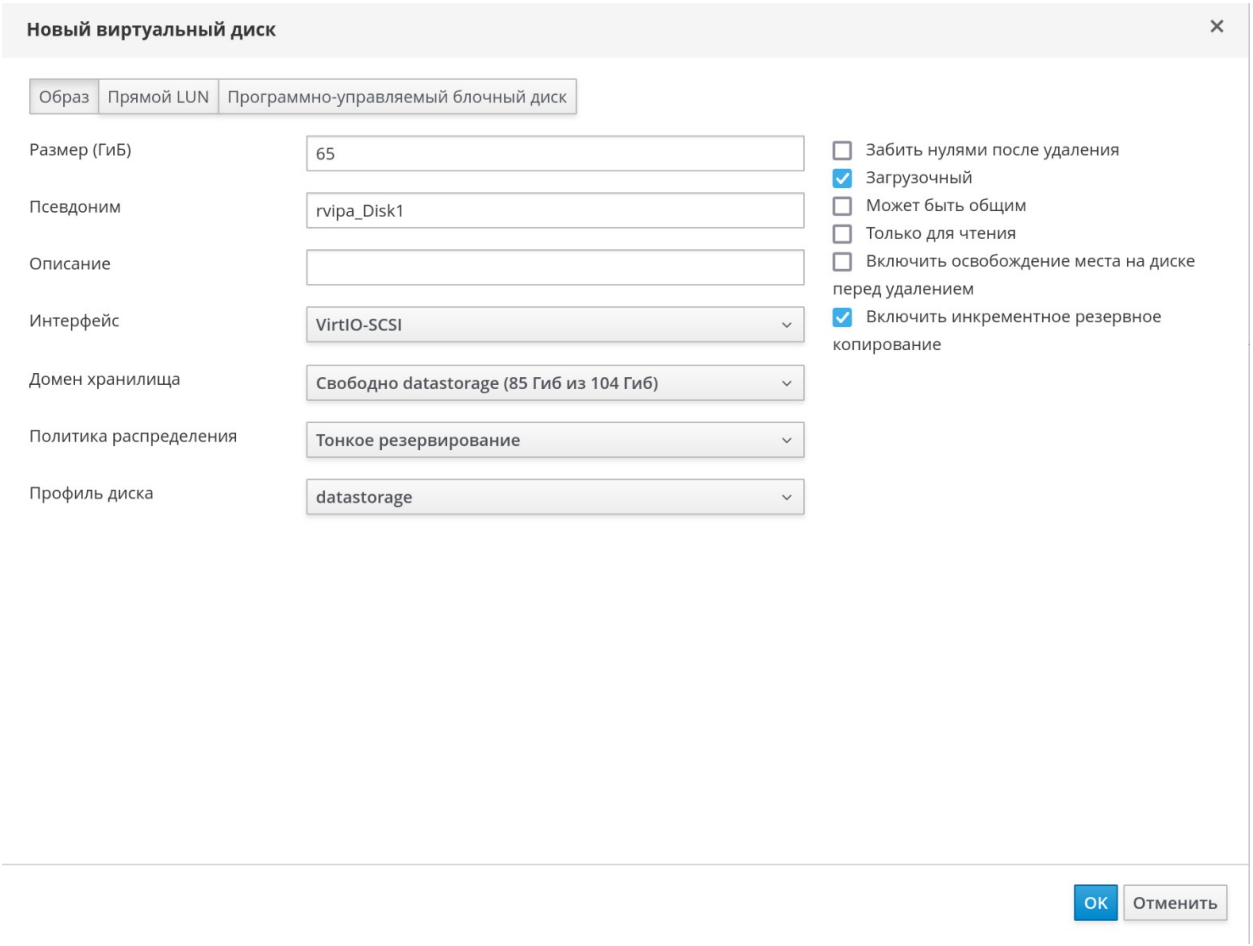

Рисунок 77 – Окно "Новый виртуальный диск"

В поле "Размер (ГиБ)" укажите размер виртуального диска не менее 62 ГБ.

После настройки опциональных параметров виртуального диска нажмите кнопку OK для сохранения указанных значений и возвращения в окно "Новая ВМ".

Далее в окне "Новая ВМ" перейдите на вкладку "Система" (рисунок 78).

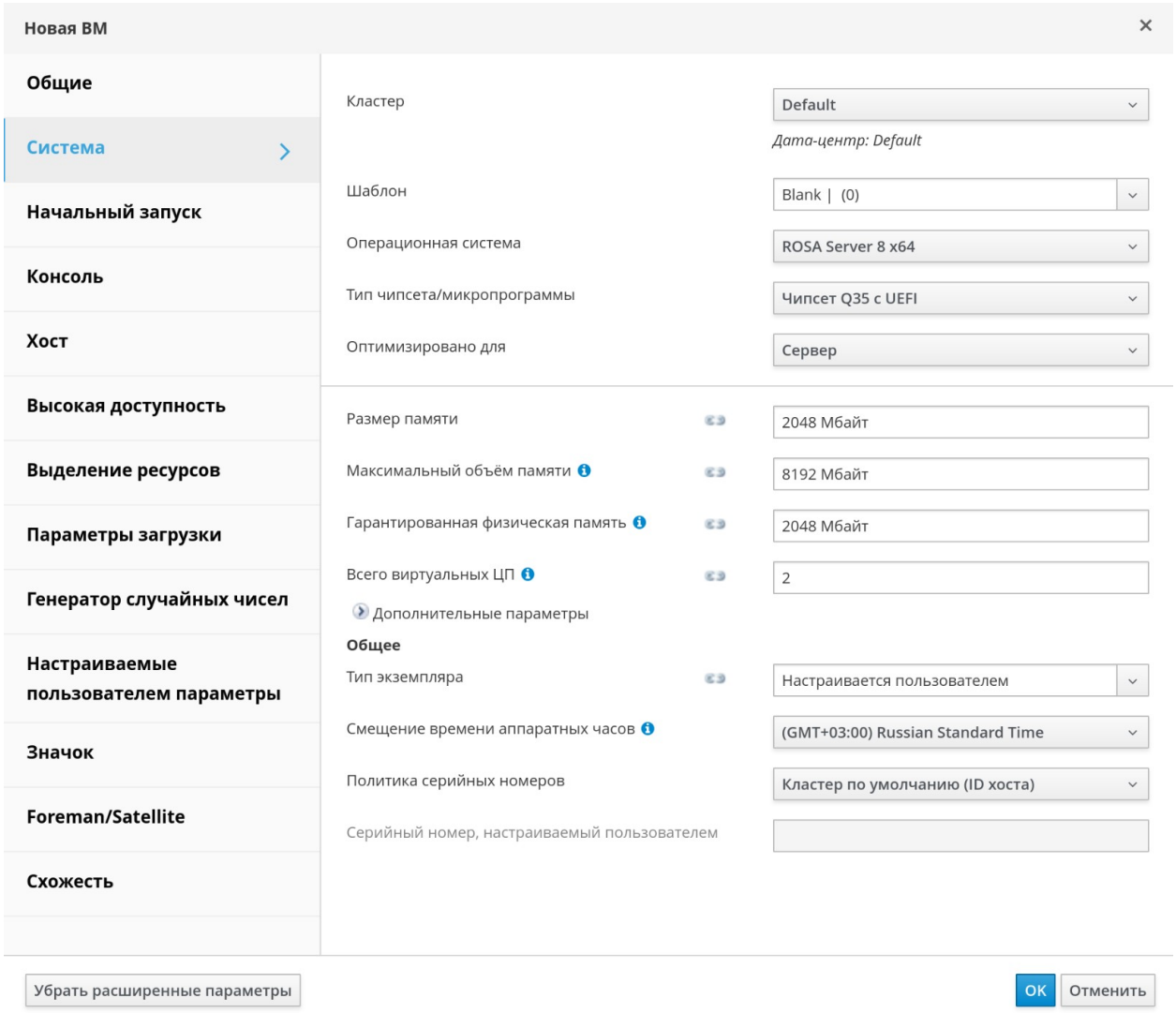

Рисунок 78 – Вкладка "Система". Укажите требуемый размер памяти и региональные настройки

В поле "Размер памяти" укажите объем используемой оперативной памяти не менее 2 ГБ. В поле "Всего виртуальных ЦП" укажите требуемое число виртуальных процессоров (ядер) (рисунок 78).

Перейдите на вкладку "Параметры загрузки" (рисунок 79).

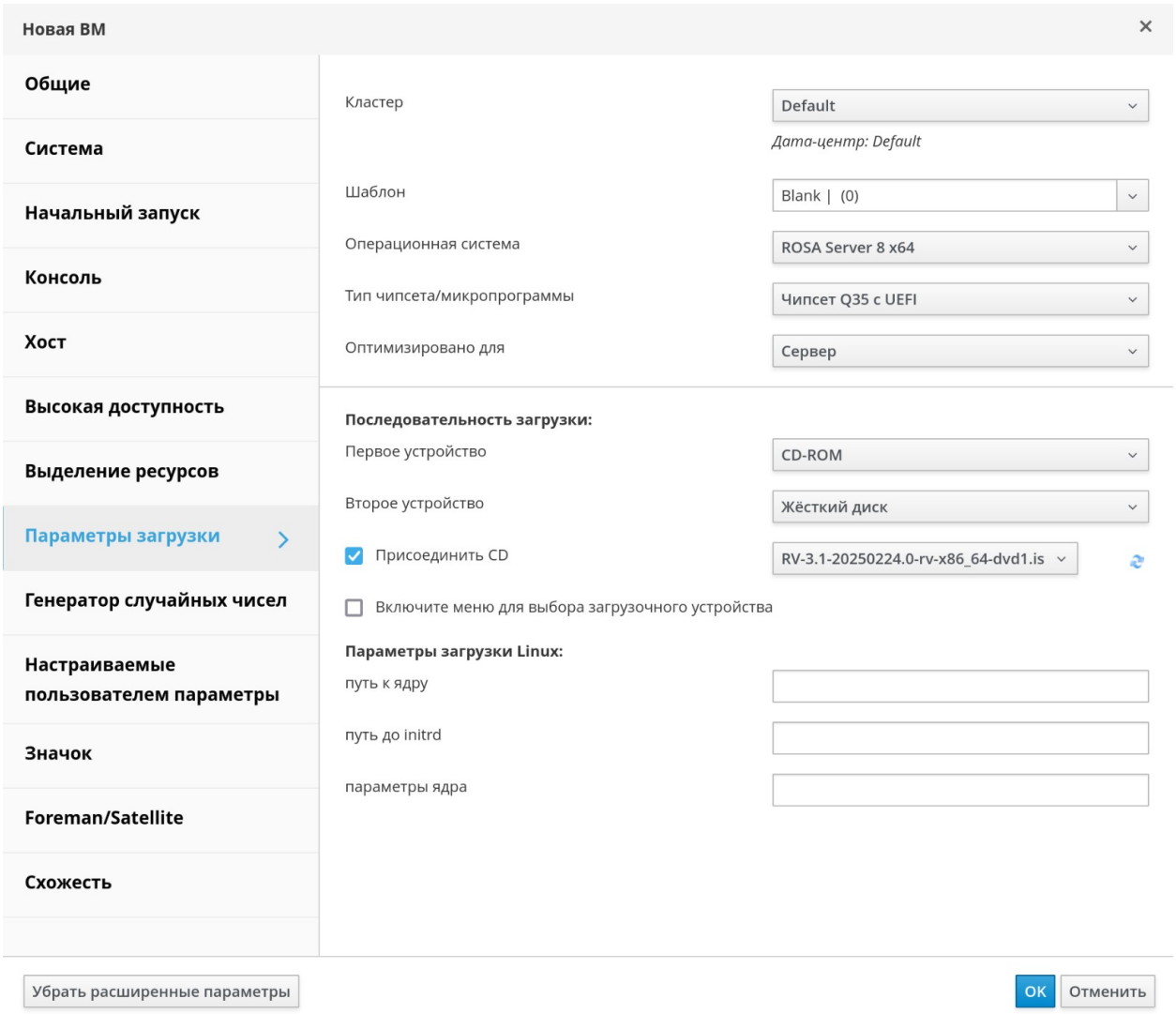

Рисунок 79 – Вкладка "Параметры загрузки"

Установите последовательность загрузки устройств. Для последующей установки ОС с загруженного образа с дистрибутивом сервера IPA выберите из выпадающего списка "Первое устройство" значение "CD-ROM", а из выпадающего списка "Второе устройство" значение "Жесткий диск" (рисунок 79).

Установите флажок "Присоединить CD" и выберите из выпадающего списка образ с дистрибутивом (файл RV-3.1-20250224.0-rv-x86_64-dvd1.iso).

Для применения всех сделанных настроек и создания новой ВМ нажмите кнопку OK.

В результате на портале администрирования СУСВ в меню "Ресурсы → Виртуальные машины" появится новая ВМ, созданная для сервера IPA.

После создания новой ВМ настройте параметры виртуального сетевого интерфейса. Для этого во внутреннем меню ВМ нажмите кнопку Изменить и во вкладке "Общие" выберите из выпадающего списка необходимое значение (рекомендуемый вариант – "ovirtmgmt").

Для перехода к процессу установки ОС на сервер IPA выберите созданную ВМ и нажмите кнопку Запустить, а после изменения состояния ВМ нажмите кнопку Консоль.

На экране появится интерфейс программы установки ОС.

3.8.2 Установка ОС на сервер IPA

Процесс установки ОС на сервер IPA во многом аналогичен процедуре установки ОС гипервизора, которая полностью и подробно приведена в разделе 3.2.

Для установки ОС загрузите физический сервер или созданную ВМ с носителя с дистрибутивом сервера IPA.

На экране последовательно появятся меню программы установки, окно приветствия и меню "Сводка установки", которое содержит различные секции для настройки параметров установки (рисунок 80).

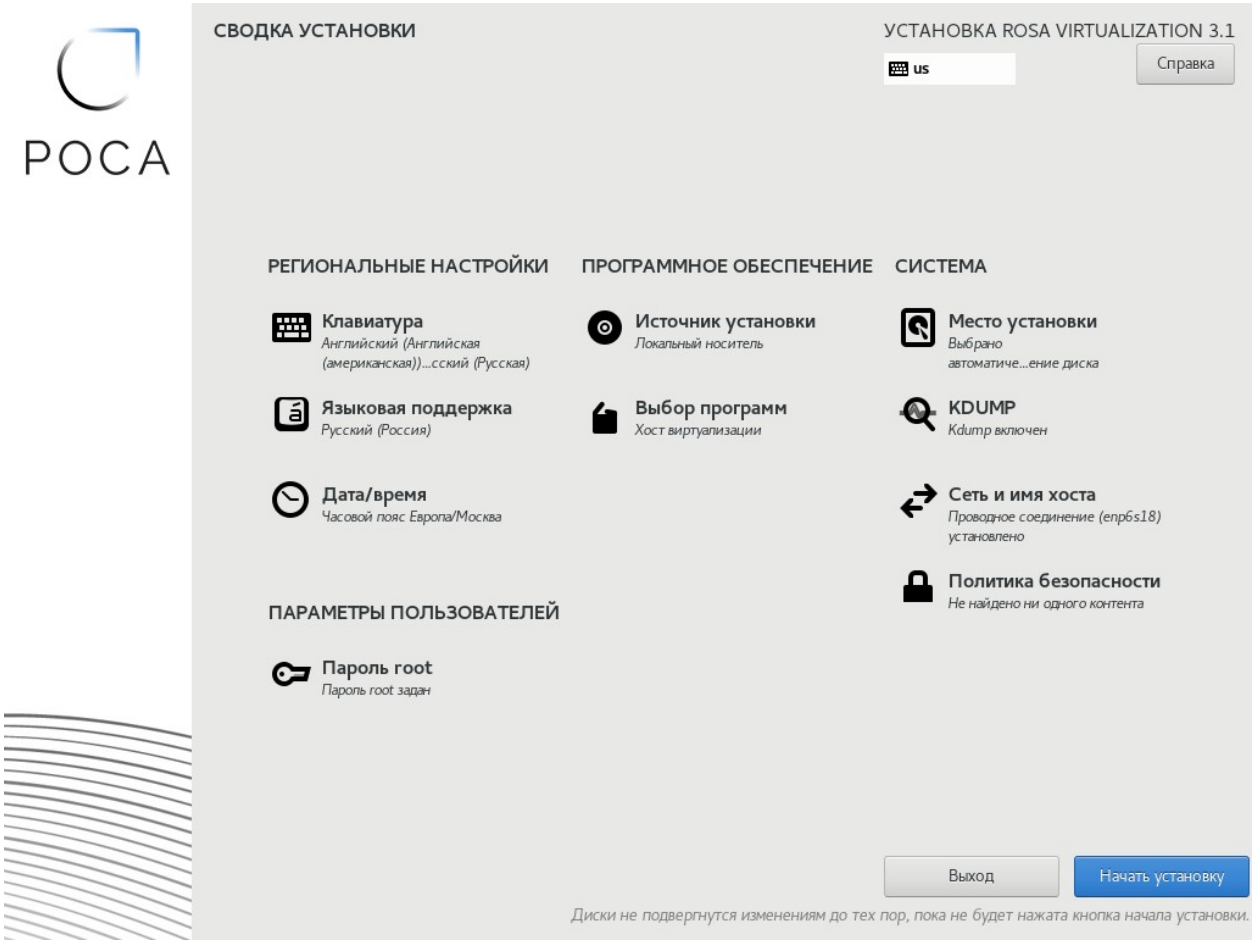

Рисунок 80 – Сводка установки ROSA Virtualization

Под наименованием каждой секции приводится информация о текущих параметрах, настроенных автоматически программой установки.

Нажмите на наименование секции для перехода к интерфейсу настройки соответствующих параметров. После настройки параметров нажмите кнопку Готово для возвращения в меню "Сводка установки".

Следующие секции являются обязательными для настройки параметров установки ОС сервера IPA:

– Выбор программ;
– Целевое устройство установки;
– Сеть и имя хоста;
– Пароль root.

В секции "Выбор программ" установите переключатель "Базовое окружение" в положение "Служба каталогов (РОСА Функции контроллера домена)" (рисунок 81) для установки соответствующего базового ПО в систему.

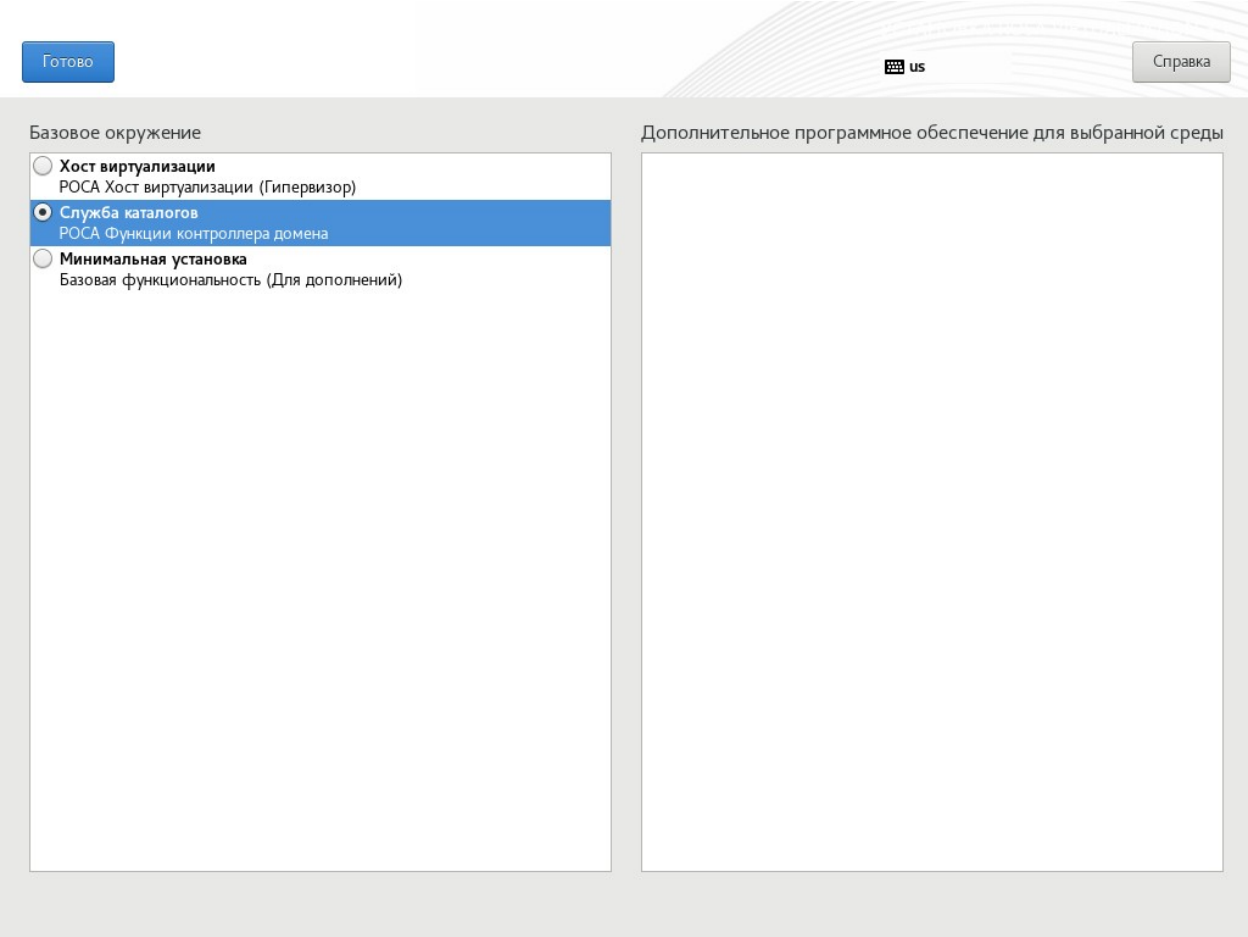

Рисунок 81 – Выбор базового ПО для установки: "Служба каталогов – РОСА Функции контроллера домена"

В секции "Целевое устройство установки" выберите необходимый диск и установите переключатель "Конфигурация устройств хранения данных" в положение "Автоматически".

В секции "Сеть и имя хоста" задайте полное доменное имя сервера IPA (например, ipa.rosa.lan), подключите необходимый сетевой интерфейс и настройте параметры сетевого соединения: DHCP или статические значения IP-адреса (например, 10.10.20.8), маски сети (255.255.255.0), шлюза по умолчанию (10.10.20.1) и сервера DNS (10.10.20.1).

В секции "Пароль root" установите пароль для учетной записи суперпользователя root.

После настройки всех обязательных параметров нажмите кнопку Начать установку для старта процесса установки ОС (рисунок 80).

После завершения процесса установки нажмите кнопку Перезагрузка системы (рисунок 82).

Рисунок 82 – Окно с информацией о завершении установки системы и кнопкой перезагрузки системы

На физическом сервере извлеките DVD- или USB-накопитель, с которого выполнялась установка, а в настройках ВМ установите приоритет загрузки с жесткого диска.

После перезагрузки ОС на экране появится строка приглашения командного интерпретатора для входа в систему и дальнейшего выполнения сценария установки и настройки ПО сервера IPA. Вход в систему осуществляется с использованием логина и пароля учетной записи суперпользователя root (рисунок 83).

Рисунок 83 – Вход в систему – системная консоль

3.8.3 Выполнение сценария установки ПО сервера IPA

Установка и настройка ПО сервера IPA осуществляется консольной утилитой (сценарием установки) ipa-server-install.

Примечание – Сценарий установки ipa-server-install создает файл журнала /var/log/ipaserver-install.log. В случае неудачной установки можно просмотреть записи журнала для выявления проблемы в процессе установки.

3.8.3.1 Рекомендованная конфигурация для установки сервера IPA

Рекомендуется установить сервер IPA со встроенной службой DNS и со встроенным центром сертификации CA в качестве корневого удостоверяющего центра. Данные параметры являются значениями по умолчанию.

3.8.3.2 Запуск сценария установки сервера IPA

Для запуска интерактивного сценария установки сервера IPA осуществите вход в систему от имени учетной записи суперпользователя root и выполните следующую консольную команду:

```
    # ipa-server-install

    The log file for this installation can be found in
/var/log/ipaserver-install.log
    ==============================================================
==================
    This program will set up the IPA Server.
    Version 4.9.13

    This includes:
      * Configure a stand-alone CA (dogtag) for certificate
management
      * Configure the NTP client (chronyd)
      * Create and configure an instance of Directory Server
      * Create and configure a Kerberos Key Distribution Center
(KDC)
      * Configure Apache (httpd)
      * Configure SID generation
      * Configure the KDC to enable PKINIT

    To accept the default shown in brackets, press the Enter
key.
```

Сценарий установки выведет справочную информацию о действиях, которые будут выполнены, а затем предложит настроить встроенную службу DNS.

Для подтверждения согласия настройки встроенной службы DNS введите "yes":

```
    Do you want to configure integrated DNS (BIND)? [no]: yes
```

Далее сценарий установки предложит определенные значения по умолчанию для следующих параметров:

– имя хоста сервера IPA (host name);

– имя домена (domain name);
– имя области Kerberos (realm name):

```
Server host name [ipa.rosa.lan]:
Please confirm the domain name [rosa.lan]:
Please provide a realm name [ROSA.LAN]:
```

Чтобы принять предложенные значения по умолчанию, нажмите клавишу `Enter`.

При необходимости вы можете внести изменения в имя хоста сервера, имя домена, имя области Kerberos.

Для изменения параметра по умолчанию введите необходимое значение, соответствующее установке в вашем ЦОД, и затем нажмите клавишу `Enter`.

Примечание – Указанные выше имя хоста сервера IPA, имя домена и имя области Kerberos являются **примером**. При установке их необходимо заменить на используемые в организации.

Установите (введите и подтвердите) пароли для:

– суперпользователя службы каталогов LDAP (Directory Manager);
– пользовательской административной учетной записи admin сервера IPA (IPA admin):

```
Certain directory server operations require an
administrative user.
This user is referred to as the Directory Manager and has
full access
to the Directory for system management tasks and will be
added to the
instance of directory server created for IPA.
The password must be at least 8 characters long.

Directory Manager password:
Password (confirm):

The IPA server requires an administrative user, named
"admin".
This user is a regular system account used for IPA server
administration.

IPA admin password:
```

```
Password (confirm):
```

Далее сценарий установки предложит настроить перенаправление DNS:

```
Do you want to configure DNS forwarders? [yes]:
```

Если перенаправление DNS конфигурировать не нужно, введите "no" (рекомендованная опция по умолчанию).

Для настройки перенаправления DNS нажмите клавишу `Enter` или введите "yes". Сценарий установки запросит и затем добавит IP-адреса средств перенаправления в файл /etc/named.conf.

Пример:

```
Do you want to configure DNS forwarders? [yes]: no
No DNS forwarders configured
```

Примечание – В примере выше перенаправление DNS не было сконфигурировано.

Далее сценарий установки предложит проверить, нужно ли настроить какие-либо обратные записи DNS для IP-адресов, связанных с сервером IPA. Для подтверждения нажмите клавишу `Enter` или введите "yes":

```
Do you want to search for missing reverse zones? [yes]:
```

Если в результате поиска будут обнаружены отсутствующие обратные зоны, сценарий установки спросит, нужно ли создать обратные зоны для соответствующих обратных записей DNS. Для подтверждения нажмите клавишу `Enter`:

```
Checking DNS domain 20.10.10.in-addr.arpa., please wait ...
Do you want to create reverse zone for IP 10.10.20.8 [yes]:
Please specify the reverse zone name [20.10.10.in-
addr.arpa.]: zone1
Invalid reverse zone zone1 for IP address 10.10.20.8
Please specify the reverse zone name [20.10.10.in-
addr.arpa.]:
Checking DNS domain 20.10.10.in-addr.arpa., please wait ...
Using reverse zone(s) 20.10.10.in-addr.arpa.
```

Далее сценарий установки предложит настроить доменное имя NetBIOS:

```
Trust is configured but no NetBIOS domain name found,
setting it now.
Enter the NetBIOS name for the IPA domain.
```

```
    Only up to 15 uppercase ASCII letters, digits and dashes are
allowed.
    Example: EXAMPLE.

    NetBIOS domain name [ROSA]:
```

Введите доменное имя NetBIOS, для подтверждения нажмите клавишу `Enter`.

Опционально вы можете также настроить сервер NTP (NTP server) или пул адресов серверов точного времени:

```
    Do you want to configure chrony with NTP server or pool
address? [no]:
```

Сценарий установки выведет в консоль выбранные параметры настройки сервера IPA. Проверьте указанные настройки на соответствие требуемым настройкам:

```
    The IPA Master Server will be configured with:
    Hostname:       ipa.rosa.lan
    IP address(es): 10.10.20.8
    Domain name:    rosa.lan
    Realm name:     ROSA.LAN

    The CA will be configured with:
    Subject DN:   CN=Certificate Authority,O=ROSA.LAN
    Subject base: O=ROSA.LAN
    Chaining:     self-signed

    BIND DNS server will be configured to serve IPA domain with:
    Forwarders:       No forwarders
    Forward policy:   only
    Reverse zone(s):  20.10.10.in-addr.arpa.
```

Для подтверждения всех сделанных настроек конфигурации сервера IPA введите "yes":

```
    Continue to configure the system with these values? [no]:
yes
```

Сценарий приступит к установке ПО сервера IPA в соответствии с заданной конфигурацией.

После завершения установки ПО сервера IPA на экране появится соответствующее сообщение, а также сценарий установки порекомендует сделать резервную копию сертификата центра сертификации CA и убедиться в том, что требуемые сетевые порты сервера IPA открыты для входящих соединений:

```
    The following operations may take some minutes to complete.
    Please wait until the prompt is returned.

    Adding [10.10.20.8 ipa.rosa.lan] to your /etc/hosts file
    Disabled p11-kit-proxy
    Synchronizing time
    No SRV records of NTP servers found and no NTP server or
pool address was provided.
    Using default chrony configuration.
    Attempting to sync time with chronyc.
    Time synchronization was successful.
    Configuring directory server (dirsrv). Estimated time: 30
seconds
      [1/43]: creating directory server instance
    Validate installation settings ...
    Create file system structures ...
    Perform SELinux labeling ...
    Setting label dirsrv_var_lib_t in seLinux file context
/var/lib/dirsrv/slapd-ROSA-LAN/bak.
    Setting label dirsrv_config_t in seLinux file context
/etc/dirsrv/slapd-ROSA-LAN.
    Setting label dirsrv_var_lib_t in seLinux file context
/var/lib/dirsrv/slapd-ROSA-LAN/db.
    Setting label dirsrv_var_lib_t in seLinux file context
/var/lib/dirsrv/slapd-ROSA-LAN/ldif.
    Setting label dirsrv_var_lock_t in seLinux file context
/var/run/lock/dirsrv/slapd-ROSA-LAN.
    Setting label dirsrv_var_log_t in seLinux file context
/var/log/dirsrv/slapd-ROSA-LAN.
    Setting label dirsrv_tmpfs_t in seLinux file context
/dev/shm/slapd-ROSA-LAN.
```

```
    Setting label dirsrv_var_run_t in seLinux file context
/var/run/dirsrv.
    Setting label dirsrv_config_t in seLinux file context
/etc/dirsrv/slapd-ROSA-LAN/schema.
    Create database backend: dc=rosa,dc=lan ...
    Perform post-installation tasks ...
      [2/43]: tune ldbm plugin
      [3/43]: adding default schema
    . . .
    . . .
    Done configuring the web interface (httpd).
    Configuring Kerberos KDC (krb5kdc)
      [1/1]: installing X509 Certificate for PKINIT
    Done configuring Kerberos KDC (krb5kdc).
    Applying LDAP updates
    Upgrading IPA:. Estimated time: 1 minute 30 seconds
      [1/10]: stopping directory server
      [2/10]: saving configuration
      [3/10]: disabling listeners
      [4/10]: enabling DS global lock
      [5/10]: disabling Schema Compat
      [6/10]: starting directory server
      [7/10]: upgrading server
      [8/10]: stopping directory server
      [9/10]: restoring configuration
      [10/10]: starting directory server
    Done.
    Restarting the KDC
    dnssec-validation yes
    Configuring DNS (named)
      [1/12]: generating rndc key file
      [2/12]: adding DNS container
      [3/12]: setting up our zone
      [4/12]: setting up reverse zone
      [5/12]: setting up our own record
      [6/12]: setting up records for other masters
      [7/12]: adding NS record to the zones
```

```
      [8/12]: setting up kerberos principal
      [9/12]: setting up named.conf
    created new /etc/named.conf
    created named user config "/etc/named/ipa-ext.conf"
    created named user config "/etc/named/ipa-options-ext.conf"
    created named user config "/etc/named/ipa-logging-ext.conf"
      [10/12]: setting up server configuration
      [11/12]: configuring named to start on boot
      [12/12]: changing resolv.conf to point to ourselves
    Done configuring DNS (named).
    Restarting the web server to pick up resolv.conf changes
    Configuring DNS key synchronization service (ipa-
dnskeysyncd)
      [1/7]: checking status
      [2/7]: setting up bind-dyndb-ldap working directory
      [3/7]: setting up kerberos principal
      [4/7]: setting up SoftHSM
      [5/7]: adding DNSSEC containers
      [6/7]: creating replica keys
      [7/7]: configuring ipa-dnskeysyncd to start on boot
    Done configuring DNS key synchronization service (ipa-
dnskeysyncd).
    Restarting ipa-dnskeysyncd
    Restarting named
    Updating DNS system records
    Configuring SID generation
      [1/8]: creating samba domain object
      [2/8]: adding admin(group) SIDs
      [3/8]: adding RID bases
      [4/8]: updating Kerberos config
    "dns_lookup_kdc" already set to "true", nothing to do.
      [5/8]: activating sidgen task
      [6/8]: restarting Directory Server to take MS PAC and LDAP
plugins changes into account
      [7/8]: adding fallback group
      [8/8]: adding SIDs to existing users and groups
```

```
    This step may take considerable amount of time, please
wait..
    Done.
    Restarting the KDC
    Configuring client side components
    This program will set up IPA client.
    Version 4.9.13

    Using existing certificate "/etc/ipa/ca.crt".
    Client hostname: ipa.rosa.lan
    Realm: ROSA.LAN
    DNS Domain: rosa.lan
    IPA Server: ipa.rosa.lan
    BaseDN: dc=rosa,dc=lan

    Configured /etc/sssd/sssd.conf
    Systemwide CA database updated.
    Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
    Adding SSH public key from
/etc/ssh/ssh_host_gost2001_key.pub
    Adding SSH public key from
/etc/ssh/ssh_host_gost2012_512_key.pub
    Adding SSH public key from
/etc/ssh/ssh_host_gost2012_256_key.pub
    Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
    Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
    SSSD enabled
    Configured /etc/openldap/ldap.conf
    Configured /etc/ssh/ssh_config
    Configured /etc/ssh/sshd_config
    Configuring rosa.lan as NIS domain.
    Client configuration complete.
    The ipa-client-install command was successful

    ==========================================================
==================
    Setup complete
```

```
    Next steps:
            1. You must make sure these network ports are open:
                    TCP Ports:
                      * 80, 443: HTTP/HTTPS
                      * 389, 636: LDAP/LDAPS
                      * 88, 464: kerberos
                      * 53: bind
                    UDP Ports:
                      * 88, 464: kerberos
                      * 53: bind
                      * 123: ntp

            2. You can now obtain a kerberos ticket using the
command: "kinit admin"
                This ticket will allow you to use the IPA tools
(e.g., ipa user-add)
                and the web user interface.

    Be sure to back up the CA certificates stored in
/root/cacert.p12
    These files are required to create replicas. The password
for these
    files is the Directory Manager password
    The ipa-server-install command was successful
```

Примечание – Часть вывода в консоль в примере выше была опущена. Справочно приводятся начальная и конечная часть вывода в консоль с подтверждением успешности установки сервера IPA.

Сообщение:

```
    The ipa-server-install command was successful
```

свидетельствует о том, что установка прошла успешно.

3.8.3.3 Инициализация учетной записи администратора сервера IPA и настройка параметров учетной записи

3.8.3.3.1 Инициализация учетной записи администратора

Для получения билета Kerberos для учетной записи администратора admin необходимо выполнить команду `kinit` с указанием принципала. `kinit` получает и кэширует начальный билет на выдачу билетов для принципала.

Выполните в консоли сервера IPA команду:

```
# kinit admin
```

для получения билета Kerberos для учетной записи администратора admin. Далее необходимо подтвердить полномочия администратора, введя его пароль, например:

```
# kinit admin
Password for admin@ROSA.LAN:
```

3.8.3.3.2 Проверка учетной записи администратора

Для проверки корректной работы сервера и наличия учетной записи администратора используйте команду:

```
ipa user-find admin
```

которая осуществляет поиск нужного пользователя и вывод базовых параметров этой учетной записи.

Пример:

```
# ipa user-find admin
---------------------------------------
установлено соответствие 1 пользователя
---------------------------------------
  Имя учётной записи пользователя: admin
  Фамилия: Administrator
  Домашний каталог: /home/admin
  Оболочка входа: /bin/bash
  Псевдоним учётной записи: admin@ROSA.LAN, root@ROSA.LAN
  UID: 702400000
  ID группы: 702400000
  Учётная запись отключена: False
--------------------------------
Количество возвращённых записей 1
```

```
------------------------------
```

В данном примере была обнаружена учетная запись admin. Учетная запись включена (не заблокирована).

Примечание – Если при выполнения запроса к серверу IPA выводится сообщение об ошибке вида:

```
# ipa user-find n.petrov
ipa: ERROR: Срок действия билета истек
```

то необходимо обновить билет Kerberos, выполнив команду `kinit admin`, и подтвердить полномочия вводом пароля администратора.

Для проверки наличия действительных (валидных) билетов Kerberos можно использовать команду `klist`:

```
# klist
Ticket cache: KCM:0
Default principal: admin@ROSA.LAN

Valid starting       Expires              Service principal
03.03.2025 20:15:40  04.03.2025 19:50:10
HTTP/ipa.rosa.lan@ROSA.LAN
03.03.2025 20:13:30  04.03.2025 19:50:10
krbtgt/ROSA.LAN@ROSA.LAN
```

где:

– Default principal – принципал, используемый по умолчанию (в примере выше – admin@ROSA.LAN).

– Valid starting – дата и время, начиная с которого действует билет Kerberos (в примере выше – 03.03.2025 20:15:40).

– Expires – дата и время окончания строка действия билета Kerberos (в примере выше – 04.03.2025 19:50:10).

– Service principal – принципал службы (ресурс, к которому предоставляется доступ). В примере выше – HTTP/ipa.rosa.lan@ROSA.LAN и HTTP/ipa.rosa.lan@ROSA.LAN.

Для добавления новых пользователей в каталог пользователей сервера IPA вы можете воспользоваться консольной утилитой:

```
# ipa user-add
```

или использовать веб-интерфейс сервера IPA.

3.8.3.3.3 Параметры команды добавления нового пользователя сервера IPA

Для получения списка актуальных параметров при добавлении нового пользователя можно использовать команду `ipa user-add –help`:

```
# ipa user-add --help
Usage: ipa [global-options] user-add LOGIN [options]

Добавить нового пользователя.
Options:
  -h, --help            show this help message and exit
  --first=STR           Имя
  --last=STR            Фамилия
  --cn=STR              Полное имя
  --displayname=STR     Отображаемое имя
  --initials=STR        Инициалы
  --homedir=STR         Домашний каталог
  --gecos=STR           GECOS
  --shell=STR           Оболочка входа
  --principal=PRINCIPAL
                        Псевдоним учётной записи
  --principal-expiration=DATETIME
                        Окончание действия учётной записи
Kerberos
  --password-expiration=DATETIME
                        Окончание действия пароля
пользователя
  --email=STR           Адрес электронной почты
  --password            Запросить пароль у пользователя
  --random              Создать случайный пользовательский
пароль
  --uid=INT             ID пользователя (если не указан,
система назначит его
                        самостоятельно)
  --gidnumber=INT       ID группы
  --street=STR          Адрес
  --city=STR            Город
```

```
      --state=STR           Область/республика
      --postalcode=STR      Индекс
      --phone=STR           Номер телефона
      --mobile=STR          Номер мобильного телефона
      --pager=STR           Номер пейджера
      --fax=STR             Номер факса
      --orgunit=STR         Отдел
      --title=STR           Должность
      --manager=STR         Руководитель
      --carlicense=STR      Номер автомобиля
      --sshpubkey=STR       Открытый ключ SSH
      --user-auth-type=["password", "radius", "otp", "pkinit",
"hardened", "idp"]
                            Поддерживаемые типы аутентификации
пользователей
      --class=STR           Категория пользователей (семантика
этого атрибута
                            предназначена для локального
разбора)
      --radius=STR          Конфигурация прокси RADIUS
      --radius-username=STR
                            Имя пользователя прокси RADIUS
      --idp=STR             External IdP configuration
      --idp-user-id=STR     A string that identifies the user at
external IdP
      --departmentnumber=STR
                            Номер отдела
      --employeenumber=STR  Номер сотрудника
      --employeetype=STR    Тип сотрудника
      --preferredlanguage=STR
                            Предпочитаемый язык
      --certificate=CERTIFICATE
                            Base-64 шифрованный сертификат
пользователя
      --setattr=STR         Установить атрибут для пары
имя/значение. Формат:
```

```
                              атрибут=значение. Если атрибут
многозначный,  команда
                              заменяет уже присутствующие
значения.
      --addattr=STR           Добавить пару атрибут/значение.
Формат:
                              атрибут=значение. Атрибут должен
быть частью схемы.
      --noprivate             Не создавать личную группу
пользователя
      --all                   Получить и вывести все атрибуты,
возвращаемые
                              сервером. Влияет на содержимое
результата исполнения
                              команды.
      --raw                   Вывести записи в том виде, в котором
они хранятся на
                              сервере. Влияет только на формат
вывода данных.
      --no-members            Подавить обработку атрибутов
участия.
```

Пример добавления нового пользователя с логином "a.ivanov", именем "Александр", фамилией "Иванов" и отображаемым именем "Александр Иванов":

```
# ipa user-add a.ivanov \
--first="Александр" \
--last="Иванов" \
--displayname="Александр Иванов"
```

По умолчанию пользователь будет добавлен в группу "ipausers":

```
# ipa user-add a.ivanov \
> --first="Александр" \
> --last="Иванов" \
> --displayname="Александр Иванов"
--------------------------------
Добавлен пользователь "a.ivanov"
--------------------------------
```

```
  Имя учётной записи пользователя: a.ivanov
  Имя: Александр
  Фамилия: Иванов
  Полное имя: Александр Иванов
  Отображаемое имя: Александр Иванов
  Инициалы: АИ
  Домашний каталог: /home/a.ivanov
  GECOS: Александр Иванов
  Оболочка входа: /bin/sh
  Имя учётной записи: a.ivanov@ROSA.LAN
  Псевдоним учётной записи: a.ivanov@ROSA.LAN
  Адрес электронной почты: a.ivanov@rosa.lan
  UID: 702400003
  ID группы: 702400003
  Пароль: False
  Участник групп: ipausers
  Доступные ключи Kerberos: False
```

Строка "Участник групп: ipausers" показывает, что данный пользователь был добавлен в группу "ipausers".

Примечание – В примере выше новый пользователь с логином "a.ivanov" был добавлен в каталог пользователей без указания пароля и срока окончания действия пароля. Для возможности успешного входа в систему должен быть задан пароль учетной записи и указан срок окончания действия пароля с "датой/временем", которые наступят позднее.

3.8.3.3.4 Добавление или смена пароля пользователя

Для добавления или смены пароля пользователя необходимо использовать команду:

```
ipa user-mod user_name –password
```

где "user_name" – это имя пользователя.

Пример:

```
# ipa user-mod a.ivanov --password
Пароль:
Введите Пароль ещё раз для проверки:
------------------------------
Изменён пользователь "a.ivanov"
------------------------------
```

```
  Имя учётной записи пользователя: a.ivanov
  Имя: Александр
  Фамилия: Иванов
  Домашний каталог: /home/a.ivanov
  Оболочка входа: /bin/sh
  Имя учётной записи: a.ivanov@ROSA.LAN
  Псевдоним учётной записи: a.ivanov@ROSA.LAN
  Адрес электронной почты: a.ivanov@rosa.lan
  UID: 702400003
  ID группы: 702400003
  Учётная запись отключена: False
  Пароль: True
  Участник групп: ipausers
  Доступные ключи Kerberos: True
```

После запуска команды появится подсказка:

```
Пароль:
```

после которой необходимо указать требуемый (желаемый) пароль пользователя.

Затем появится подсказка:

```
Введите Пароль ещё раз для проверки:
```

и после неё необходимо повторно указать пароль пользователя (для проверки правильности введенного ранее пароля).

При условии, что оба введенных после подсказок пароля совпадают, пароль для пользователя будет изменён.

Информация в выводе на терминал "Пароль: True" сообщает о том, что пароль был успешно создан (изменён).

3.8.3.3.5 Изменения срока действия пароля пользователя

Для изменения срока действия пароля пользователя необходимо использовать команду:

```
ipa user-mod user_name –password-expiration
```

где "user_name" – это имя пользователя:

Укажите "дату/время" окончания действия пароля в формате "год-месяц-число час:минута:секунда" так, чтобы дата и время окончания срока

действия учетной записи наступали позднее текущего момента. Например, можно указать дату +3 месяца от текущей даты.

Пример:

```
    # ipa user-mod a.ivanov --password-expiration="2025-09-03
12:00:00Z"
    ------------------------------
    Изменён пользователь "a.ivanov"
    ------------------------------
      Имя учётной записи пользователя: a.ivanov
      Имя: Александр
      Фамилия: Иванов
      Домашний каталог: /home/a.ivanov
      Оболочка входа: /bin/sh
      Имя учётной записи: a.ivanov@ROSA.LAN
      Псевдоним учётной записи: a.ivanov@ROSA.LAN
      Окончание действия пароля пользователя: 20250903120000Z
      Адрес электронной почты: a.ivanov@rosa.lan
      UID: 702400003
      ID группы: 702400003
      Учётная запись отключена: False
      Пароль: True
      Участник групп: ipausers
      Доступные ключи Kerberos: True
```

В данном примере строка "Окончание действия пароля пользователя: 20250903120000Z" означает "Окончание действия пароля пользователя – 2025-09-03 12:00:00Z" (год 2025, месяц 09, число 03, время 12:00, 00 секунд).

При необходимости внесения изменения в срок действия пароля пользователя указанные выше действия можно повторить.

3.8.3.3.6 Изменения срока действия пароля пользователя с помощью поля krbPasswordExpiration

Для изменения срока действия пароля пользователя с помощью модификации поля "krbPasswordExpiration" необходимо использовать команду:

```
    ipa user-mod user_name –setattr=krbPasswordExpiration
```

где "user_name" – это имя пользователя.

Укажите "дату/время" окончания действия пароля в формате "год-месяц-число-час-минуты-секунды" (без дефисов), например "20250817010000Z" (год 2025, месяц 08, число 17, время 01:00, 00 секунд):

```
    # ipa user-mod n.petrov --
setattr=krbPasswordExpiration=20250817010000Z
    ------------------------------
    Изменён пользователь "n.petrov"
    ------------------------------
      Имя учётной записи пользователя: n.petrov
      Имя: Николай
      Фамилия: Петров
      Домашний каталог: /home/n.petrov
      Оболочка входа: /bin/sh
      Имя учётной записи: n.petrov@ROSA.LAN
      Псевдоним учётной записи: n.petrov@ROSA.LAN
      Окончание действия пароля пользователя: 20250817010000Z
      Адрес электронной почты: n.petrov@rosa.lan
      UID: 702400005
      ID группы: 702400005
      Учётная запись отключена: False
      Пароль: False
      Участник групп: ipausers
      Доступные ключи Kerberos: False
```

3.8.3.3.7 Проверки даты и времени окончания срока действия пароля учетной записи пользователя

Для проверки даты и времени окончания срока действия пароля учетной записи пользователя используйте команду:

```
    ipa user-show user_name --all –raw
```

где "user_name" – имя пользователя и далее фильтр по атрибуту "krbPasswordExpiration".

Пример 1:

```
    # ipa user-show a.ivanov --all --raw | grep
krbPasswordExpiration
      krbPasswordExpiration: 20250903120000Z
```

Значение поля "krbPasswordExpiration" соответствует дате и времени окончания срока действия пароля учетной записи – "20250903120000Z" (год 2025, месяц 09, число 03, время 12:00, 00 секунд).

Пример 2:

```
    # ipa user-show n.petrov --all --raw | grep
krbPasswordExpiration
      krbPasswordExpiration: 20250817010000Z
```

где "20250817010000Z" – год 2025, месяц 08, число 17, время 01:00, 00 секунд

3.8.3.3.8 Проверка наличия пользователя в каталоге IPA

Для проверки наличия пользователя в каталоге IPA необходимо выполнить в консоли команду:

```
    ipa user-find
```

Если пользователь отсутствует в каталоге, то будет выведено сообщение, что пользователь не найден:

```
    # ipa user-find n.petrov
    ---------------------------------------
    установлено соответствие 0 пользователей
    ---------------------------------------
    --------------------------------
    Количество возвращённых записей 0
    --------------------------------
```

Если пользователь присутствует в каталоге, то будет выведено сообщение с параметрами учетной записи пользователя:

```
    # ipa user-find a.ivanov
    ---------------------------------------
    установлено соответствие 1 пользователя
    ---------------------------------------
      Имя учётной записи пользователя: a.ivanov
      Имя: Александр
      Фамилия: Иванов
      Домашний каталог: /home/a.ivanov
      Оболочка входа: /bin/sh
      Имя учётной записи: a.ivanov@ROSA.LAN
      Псевдоним учётной записи: a.ivanov@ROSA.LAN
```

```
  Адрес электронной почты: a.ivanov@rosa.lan
  UID: 702400003
  ID группы: 702400003
  Учётная запись отключена: False
----------------------------------
Количество возвращённых записей 1
----------------------------------
```

Альтернативным способом запроса данных пользователя из каталогов IPA является утилита ldapsearch. Для проверки наличия пользователя в каталоге или запроса параметров учетной записи пользователя выполните команду:

```
ldapsearch -x uid=<идентификатор пользователя>
```

где идентификатор пользователя – это уникальный идентификатор пользователя в системе (UID).

Пример:

```
# ldapsearch -x uid=a.ivanov
# extended LDIF
#
# LDAPv3
# base <dc=rosa,dc=lan> (default) with scope subtree
# filter: uid=a.ivanov
# requesting: ALL
#

# a.ivanov, users, compat, rosa.lan
dn: uid=a.ivanov,cn=users,cn=compat,dc=rosa,dc=lan
objectClass: posixAccount
objectClass: ipaOverrideTarget
objectClass: top
gecos:: 0JDQu9C10LrRgdCw0L3QtNGAINCY0LLQsNC90L7Qsg==
cn:: 0JDQu9C10LrRgdCw0L3QtNGAINCY0LLQsNC90L7Qsg==
uidNumber: 702400003
gidNumber: 702400003
loginShell: /bin/sh
homeDirectory: /home/a.ivanov
ipaAnchorUUID::
OklQQTpyb3NhLmxhbjo4MzI1YWMxOC1mODUzLTExZWYtYjAxMC1iYzI0MTE3ZD
```

```
     YwNzY=
    uid: a.ivanov

    # a.ivanov, users, accounts, rosa.lan
    dn: uid=a.ivanov,cn=users,cn=accounts,dc=rosa,dc=lan
    givenName:: 0JDQu9C10LrRgdCw0L3QtNGA
    sn:: 0JjQstCw0L3QvtCy
    uid: a.ivanov
    cn:: 0JDQu9C10LrRgdCw0L3QtNGAINCY0LLQsNC90L7Qsg==
    displayName:: 0JDQu9C10LrRgdCw0L3QtNGAINCY0LLQsNC90L7Qsg==
    initials:: 0JDQmA==
    gecos:: 0JDQu9C10LrRgdCw0L3QtNGAINCY0LLQsNC90L7Qsg==
    objectClass: top
    objectClass: person
    objectClass: organizationalperson
    objectClass: inetorgperson
    objectClass: inetuser
    objectClass: posixaccount
    objectClass: krbprincipalaux
    objectClass: krbticketpolicyaux
    objectClass: ipaobject
    objectClass: ipasshuser
    objectClass: ipaSshGroupOfPubKeys
    objectClass: mepOriginEntry
    objectClass: ipantuserattrs
    loginShell: /bin/sh
    homeDirectory: /home/a.ivanov
    uidNumber: 702400003
    gidNumber: 702400003
    ipaNTSecurityIdentifier: S-1-5-21-2779713119-1389312704-
1424425367-1003

    # search result
    search: 2
    result: 0 Success

    # numResponses: 3
```

```
    # numEntries: 2
```

Если в каких-либо полях учетной записи используется русский алфавит, то вывод значения данного поля будет закодирован в кодировке base64.

Например, в выводе в консоли выше поле "displayName" закодировано в кодировке base64:

```
    displayName:: 0JDQu9C10LrRgdCw0L3QtNGAINCY0LLQsNC90L7Qsg==
```

Для декодирования содержимого поля (и его последующей проверки) в командной строке можно использовать утилиту base64.

Пример:

```
    # echo "0JDQu9C10LrRgdCw0L3QtNGAINCY0LLQsNC90L7Qsg==" |
base64 --decode
    Александр Иванов
```

В данном случае содержимое поля "displayName" ("отображаемое имя") декодируется как "Александр Иванов".

Также для декодирования кодировки base64 можно использовать утилиту openssl.

Пример:

```
    # openssl enc -base64 -d <<<
"0JDQu9C10LrRgdCw0L3QtNGAINCY0LLQsNC90L7Qsg=="
    Александр Иванов
```

Содержимое поля "displayName" ("отображаемое имя") декодируется как "Александр Иванов".

3.8.3.4 Настройка межсетевого экрана для сервера IPA

Для открытия необходимых портов сервера IPA в зоне "default" службы межсетевого экрана firewalld выполните следующую консольную команду (список требуемых портов приведен в таблице 4):

```
    # firewall-cmd --permanent --add-
port={80/tcp,443/tcp,389/tcp,\
    636/tcp,88/tcp,88/udp,464/tcp,464/udp,53/tcp,53/udp,123/udp}
```

Таблица 4 – Список требуемых портов для сервера IPA

Служба	Порты модуля	Протокол
HTTP/HTTPS	80, 443	TCP
LDAP/LDAPS	389, 636	TCP
Kerberos	88, 464	TCP и UDP
DNS	53	TCP и UDP
NTP	123	UDP

Примечания

1) Не следует беспокоиться о том, что сервер IPA использует порты 80 и 389.

2) Порт 80 (HTTP) используется для предоставления откликов протокола проверки статуса сертификата (OCSP) и списков аннулирования сертификатов (CRL). Обе программы имеют цифровую подпись и поэтому защищены от атак через посредника (man-in-the-middle).

3) Порт 389 (LDAP) использует STARTTLS и GSSAPI для шифрования.

Для применения изменений перезагрузите конфигурацию межсетевого экрана. Для этого выполните следующую консольную команду:

```
# firewall-cmd --reload
```

После установки ПО сервера IPA и настройки межсетевого экрана станет доступным вход в веб-интерфейс управления сервером IPA.

Для проверки статуса работы межсетевого экрана firewalld выполните команду:

```
[root@ipa ~]# systemctl status firewalld.service
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded
(/usr/lib/systemd/system/firewalld.service; enabled; vendor
preset: enabled)
   Active: active (running) since Mon 2025-03-03 19:47:45
MSK; 40min ago
     Docs: man:firewalld(1)
 Main PID: 735 (firewalld)
    Tasks: 3 (limit: 10622)
   Memory: 53.0M
```

```
       CGroup: /system.slice/firewalld.service
               └─735 /usr/bin/python3.6 -s /usr/sbin/firewalld
--nofork --nopid

    мар 03 19:47:44 ipa.rosa.lan systemd[1]: Starting firewalld
- dynamic firewall daemon...
    мар 03 19:47:45 ipa.rosa.lan systemd[1]: Started firewalld -
dynamic firewall daemon.
```

Статус "Active: active (running)" сообщает о том, что межсетевой экран активен.

3.8.4 Вход в веб-интерфейс сервера IPA

Для доступа к веб-интерфейсу введите в адресной строке браузера (на внешней рабочей станции) доменное имя или IP-адрес сервера IPA, например:

```
    https://ipa.rosa.lan
```

На экране появится окно авторизации интерфейса (рисунок 84).

Первичный вход в интерфейс управления сервером IPA осуществляется от имени учетной записи администратора admin. Предварительно необходимо получить билет Kerberos для учетной записи admin, выполнив в консоли команду:

```
    # kinit admin
```

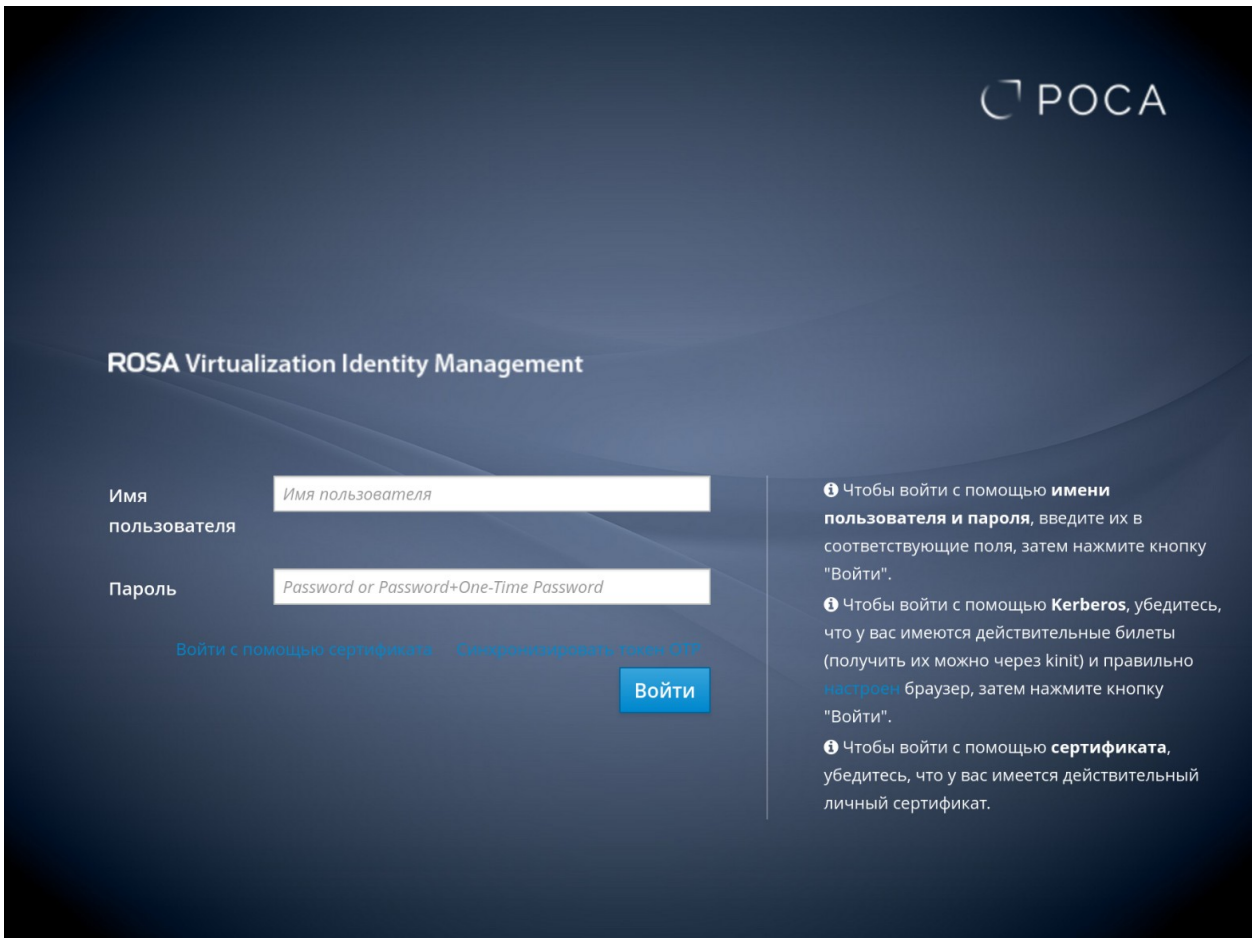

Рисунок 84 – Окно авторизации интерфейса управления сервером IPA

Для входа в интерфейс введите имя (логин) и пароль пользователя в соответствующие поля, после чего нажмите кнопку Войти.

После входа в веб-интерфейс сервера IPA будет отображена панель управления сервером IPA. По умолчанию будет открыта вкладка "Идентификация → Активные пользователи" (рисунок 85).

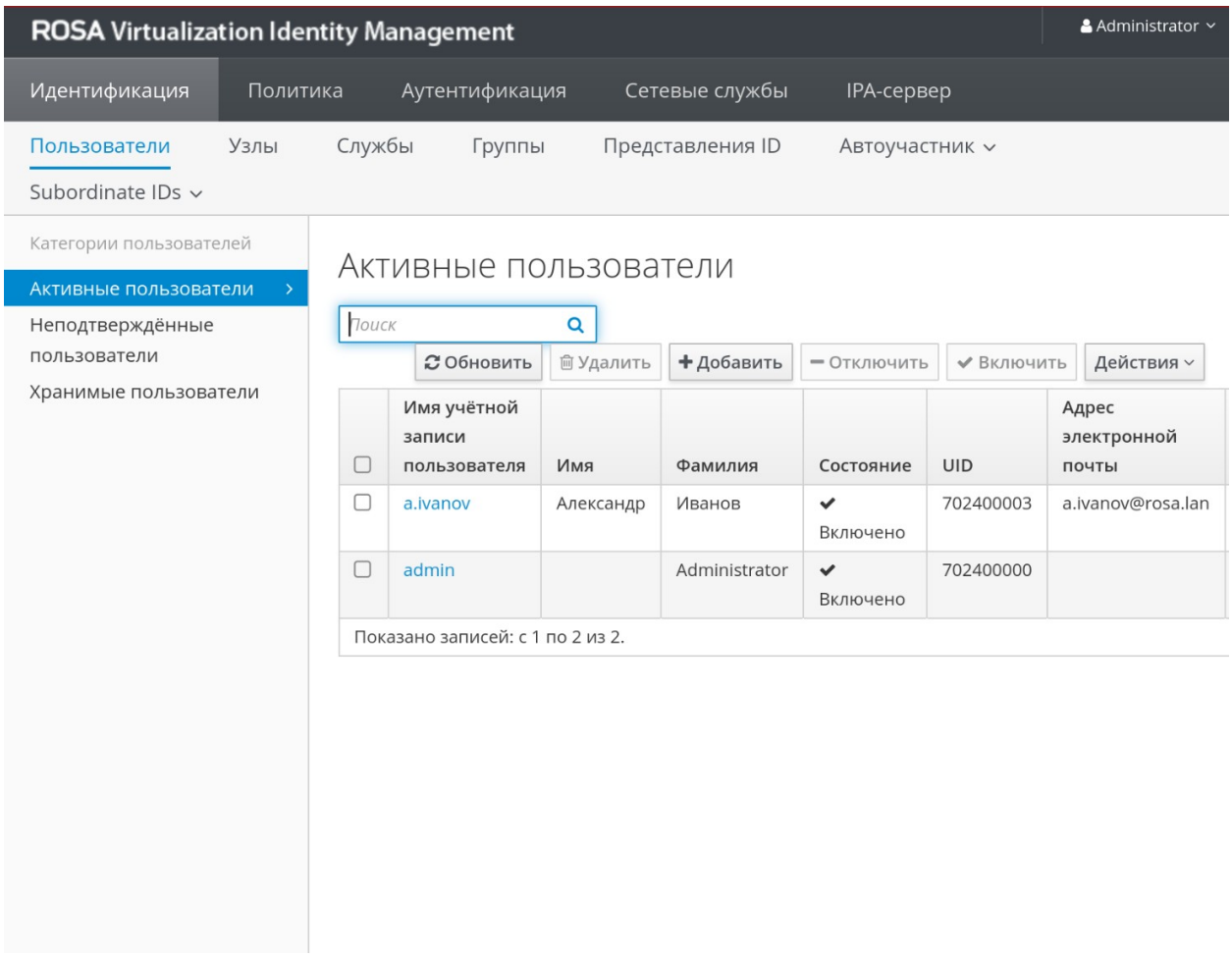

Рисунок 85 – Веб-интерфейс сервера IPA – вкладка "Идентификация" → "Активные пользователи"

Если вы уже добавили каких-либо пользователей в каталог IPA, используя интерфейс командной строки, то эти пользователи будут отображены с списке активных пользователей.

3.9 Подключение ROSA Virtualization к службе каталогов LDAP сервера IPA

Процедура подключения ROSA Virtualization к службе каталогов LDAP сервера IPA состоит из создания служебной учетной записи пользователя для выполнения запросов поиска в каталоге LDAP и входа на сервер IPA, а также из создания профиля подключения для идентификации и аутентификации доменных пользователей.

Создание служебной учетной записи пользователя осуществляется в интерфейсе управления сервером IPA (п. 3.9.1).

Создание профиля подключения осуществляется в веб-интерфейсе (п. 3.9.2) или консоли СУСВ (п. 3.9.3).

3.9.1 Создание служебной учетной записи пользователя с использованием веб-интерфейса

Для создания учетной записи пользователя выполните вход в интерфейс управления сервером IPA от имени учетной записи администратора admin.

3.9.1.1 Добавление новой учетной записи пользователя

В разделе "Идентификация" и в меню "Пользователи" выберите пункт "Активные пользователи". На экране появится соответствующая страница интерфейса, содержащая список активных пользователей (рисунок 85).

Нажмите кнопку Добавить и задайте логин для нового пользователя – сервисной учетной записи (например, "susvengine") (рисунок 86).

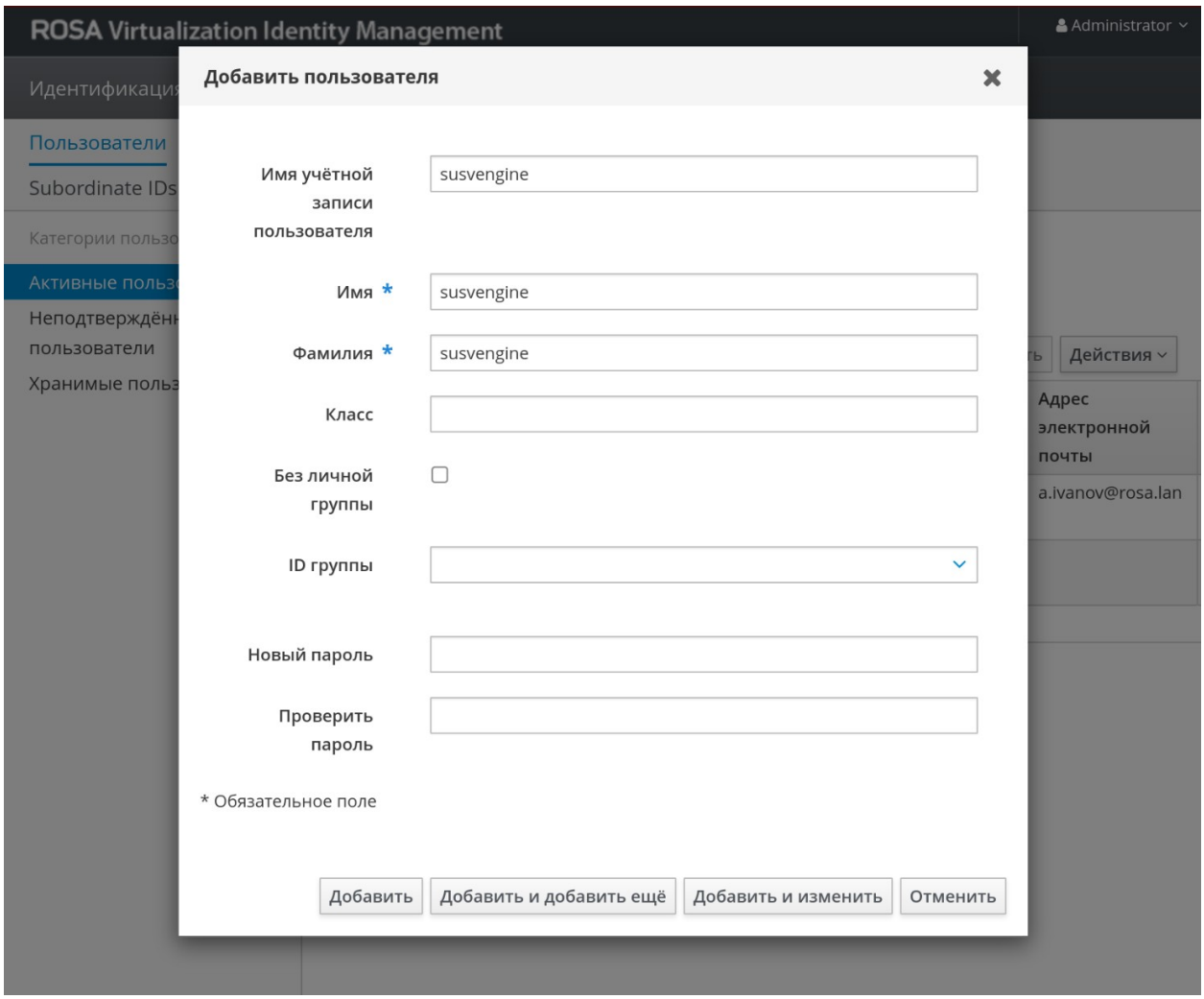

Рисунок 86 – Добавление нового пользователя – сервисной учетной записи

Примечание – Данная учетная запись является сервисной, т.е. она не соответствует ни одному человеку и используется исключительно для синхронизации сервисов СУСВ с корпоративным сервером LDAP.

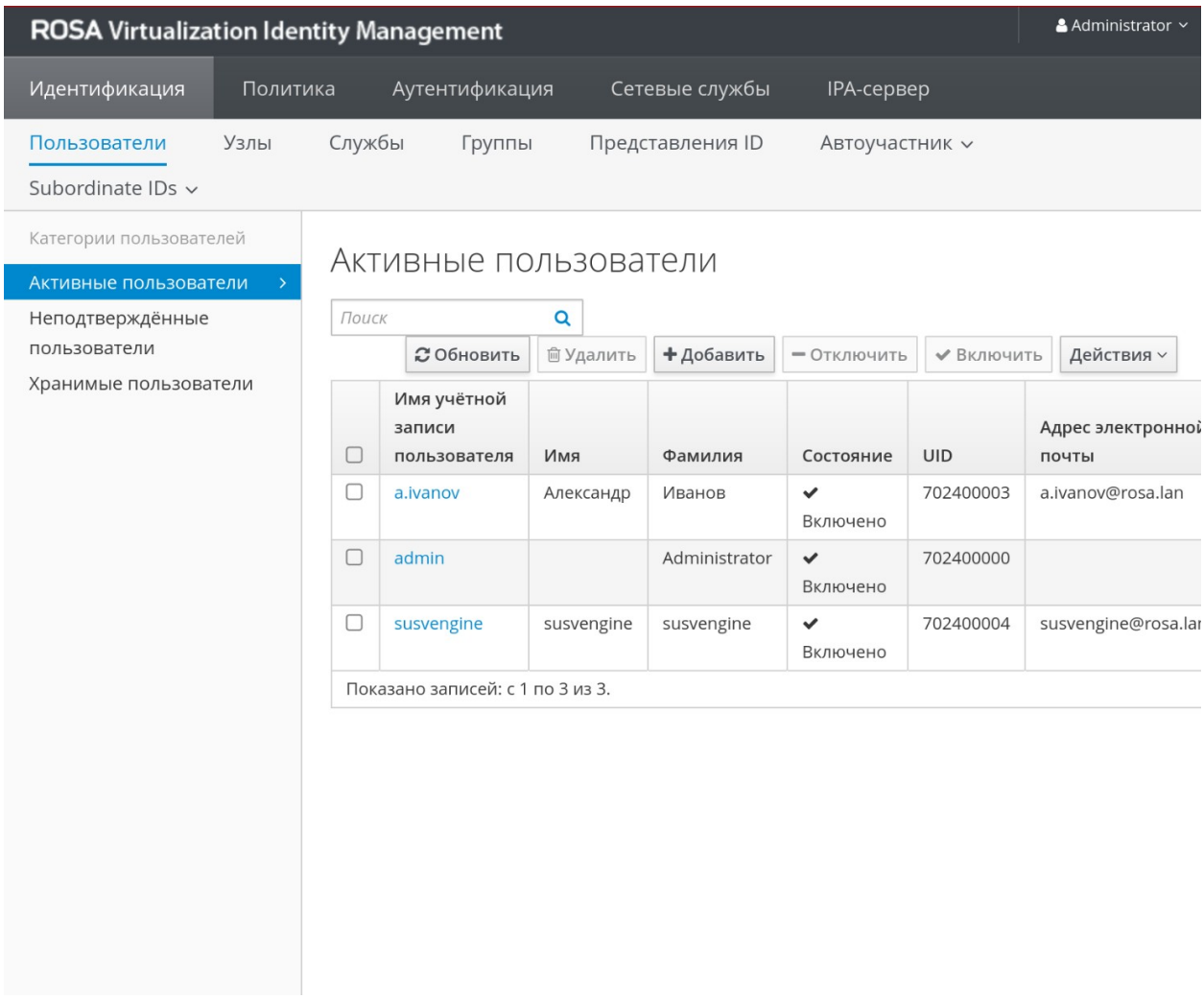

Рисунок 87 – Активные пользователи IPA, с добавленной сервисной учетной записью susvengine

3.9.1.2 Добавление учетной записи пользователя в группы

Для добавления учетной записи пользователя susvengine в группы admins и editors нажмите на ссылку с именем пользователя "susvengine" и в открывшемся меню с параметрами перейдите на вкладку "Группы пользователей" (рисунок 88).

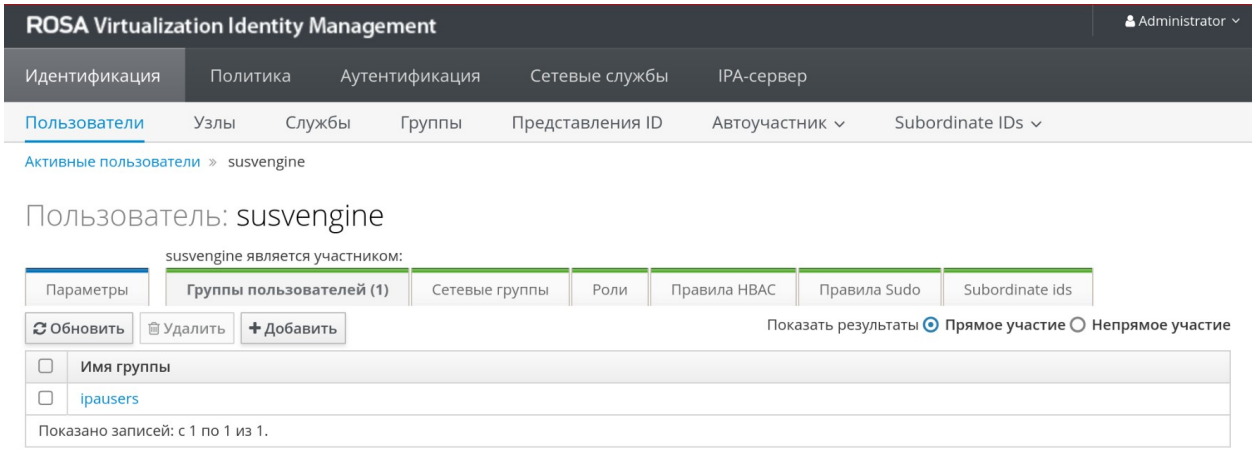

Рисунок 88 – Группы пользователей ROSA Virtualization Identity Management

Нажмите кнопку Добавить. Откроется окно с интерфейсом выбора групп для пользователя (рисунок 89).

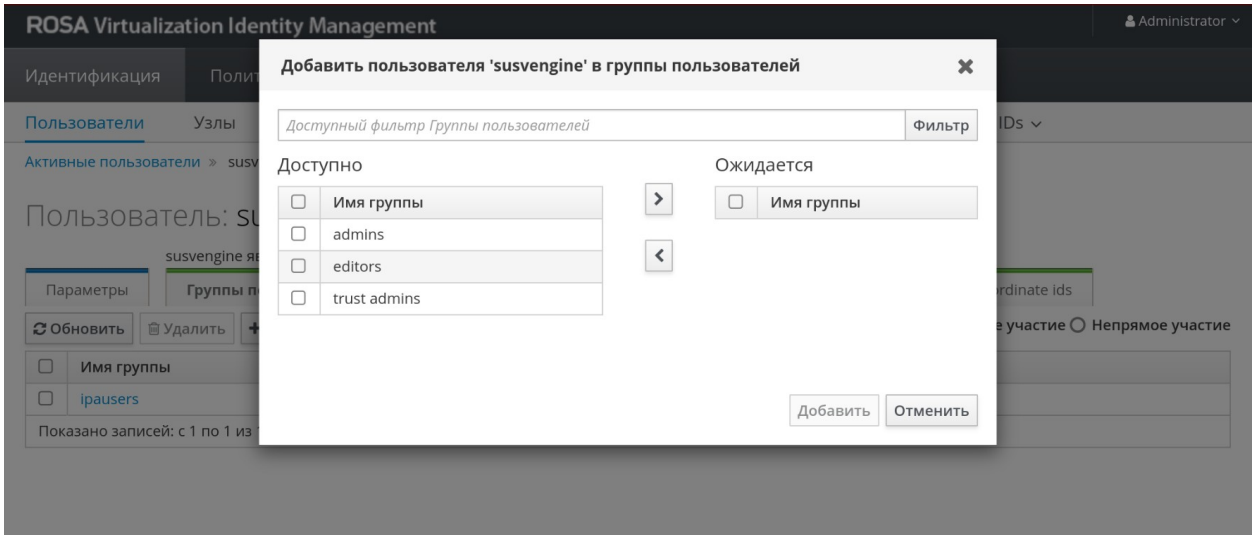

Рисунок 89 – Интерфейс выбора групп пользователей для учетной записи

В списке "Доступно" установите соответствующие флажки для выбора групп admins и editors. Нажмите кнопку переноса >. В списке "Ожидается" появятся наименования выбранных групп (рисунок 90).

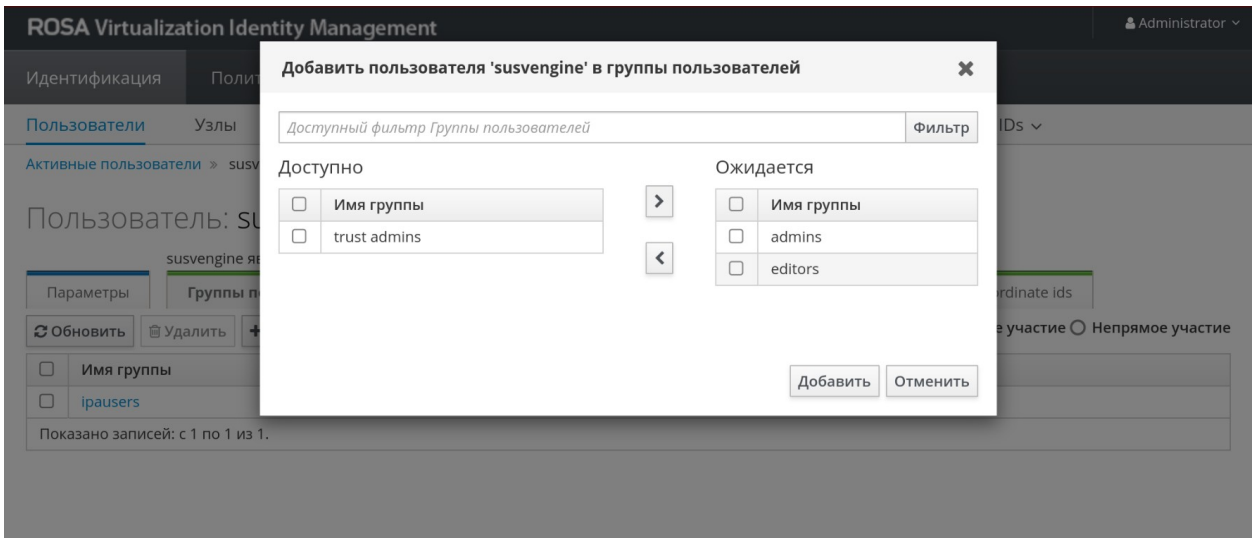

Рисунок 90 – Выбор групп admins и editors для пользователя susvengine

Для завершения процедуры выбора групп нажмите кнопку Добавить.

Учетная запись пользователя добавлена в группы admins и editors (рисунок 91).

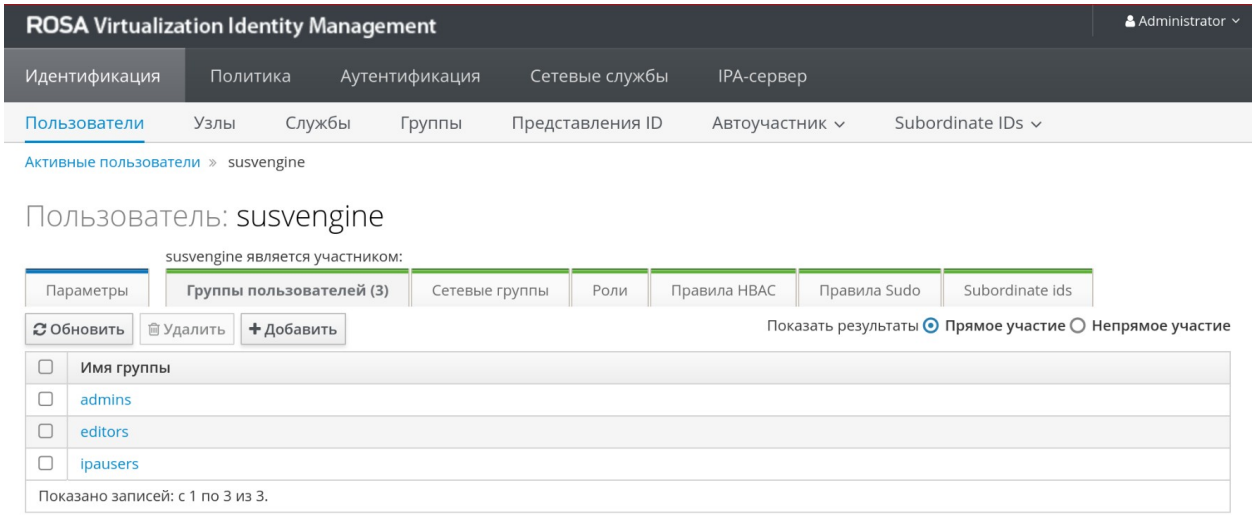

Рисунок 91 – Группы пользователя susvengine

3.9.1.3 Установка пароля для учетной записи пользователя

Для установки пароля новому пользователю перейдите на вкладку "Параметры" и из выпадающего списка, вызываемого нажатием кнопки Действия, выберите пункт "Сбросить пароль" (рисунок 92).

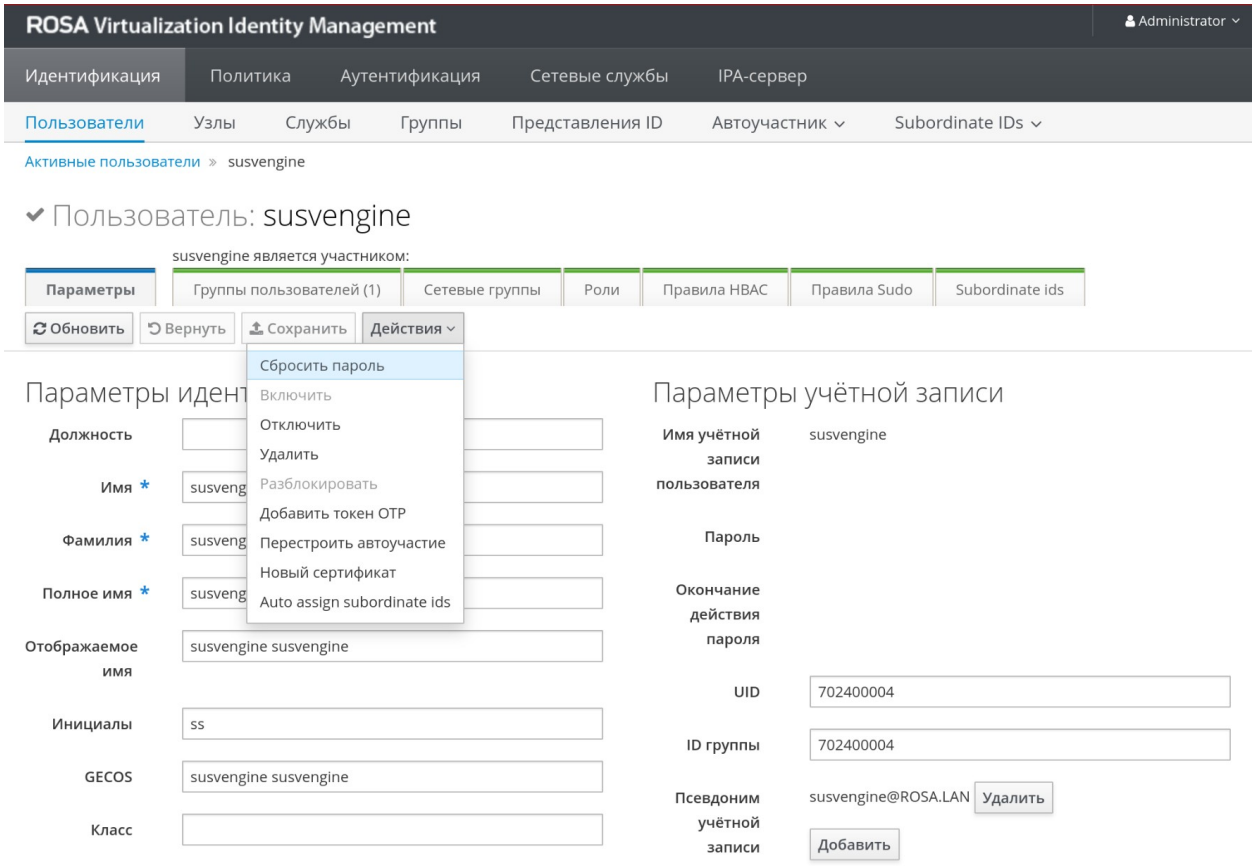

Рисунок 92 – Выбор действия "Сброс пароля" для пользователя

Содержимое полей "Пароль" и "Окончание действия пароля" не определено (поля пустые).

В поля "Новый пароль" и "Проверить пароль" открывшегося окна "Сбросить пароль" соответственно введите и подтвердите пароль для нового пользователя (рисунок 93).

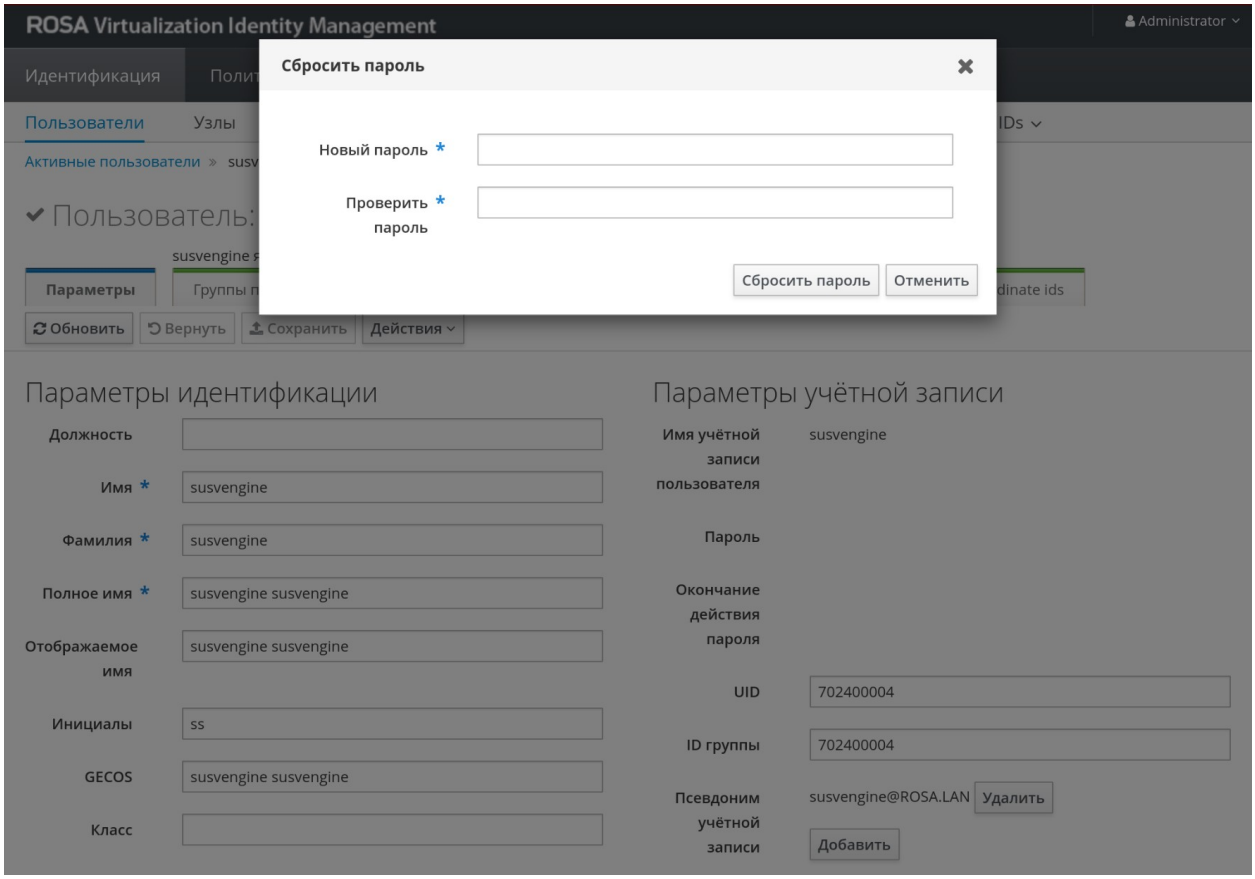

Рисунок 93 – Сброс пароля пользователя

3.9.1.4 Изменения срока действия пароля сервисной учетной записи

Для изменения срока действия пароля пользователя необходимо использовать команду:

```
ipa user-mod user_name –password-expiration
```

где "user_name" – это имя пользователя сервисной учетной записи:

Укажите "дату/время" окончания действия пароля в формате "год-месяц-число час:минута:секунда" так, чтобы дата и время окончания срока действия учетной записи наступали позднее текущего момента. Например, можно указать дату +3 месяца от текущей даты.

Пример:

```
# ipa user-mod susvengine --password-expiration="2025-10-01
12:00:00Z"
--------------------------------
Изменён пользователь "susvengine"
```

```
    ------------------------------
      Имя учётной записи пользователя: susvengine
      Имя: susvengine
      Фамилия: susvengine
      Домашний каталог: /home/susvengine
      Оболочка входа: /bin/sh
      Имя учётной записи: susvengine@ROSA.LAN
      Псевдоним учётной записи: susvengine@ROSA.LAN
      Окончание действия пароля пользователя: 20251001120000Z
      Адрес электронной почты: susvengine@rosa.lan
      UID: 702400004
      ID группы: 702400004
      Учётная запись отключена: False
      Пароль: True
      Участник групп: editors, admins, ipausers
      Доступные ключи Kerberos: True
```

В данном примере строка:

```
      Окончание действия пароля пользователя: 20251001120000Z
```

определяет год 2025, месяц 10, число 01, время 12:00, 00 секунд.

Для проверки даты и времени окончания срока действия пароля учетной записи можно воспользоваться следующей командой:

```
    # ipa user-show susvengine --all --raw | grep
krbPasswordExpiration
     krbPasswordExpiration:  20251001120000Z
```

Значение поля "krbPasswordExpiration" соответствует дате и времени окончания срока действия пароля учетной записи.

В результате выполнения описанных выше действий добавлена сервисная учетная запись "susvengine", определен пароль для учетной записи и установлен срок окончания действия пароля.

3.9.2 Создание профиля подключения к службе каталогов LDAP сервера IPA с помощью веб-интерфейса СУСВ

Для настройки профиля подключения СУСВ к службе каталогов LDAP сервера IPA с помощью веб-интерфейса используется плагин "Мастер

настройки LDAP", расположенный в административной панели СУСВ в секции "Дополнения" (рисунок 94).

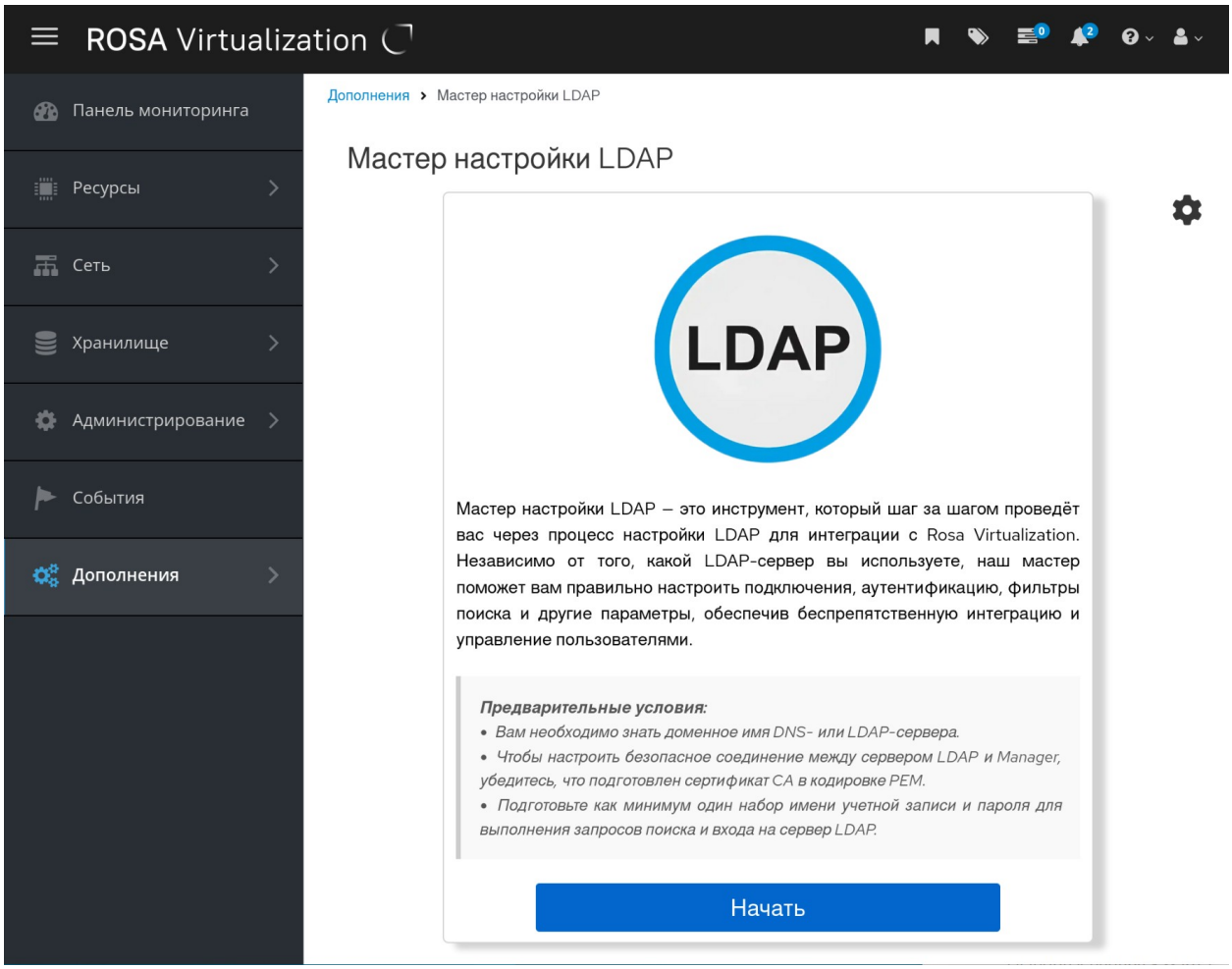

Рисунок 94 – Мастер настройки LDAP в административной панели СУСВ

Для начала работы с "Мастером настройки LDAP" нажмите на кнопку Начать.

Для настройки подключения к серверу IPA выберите (рисунок 95):

– Тип LDAP – IPA.
– Использовать DNS – нет.
– Доступный метод политики – Один сервер.

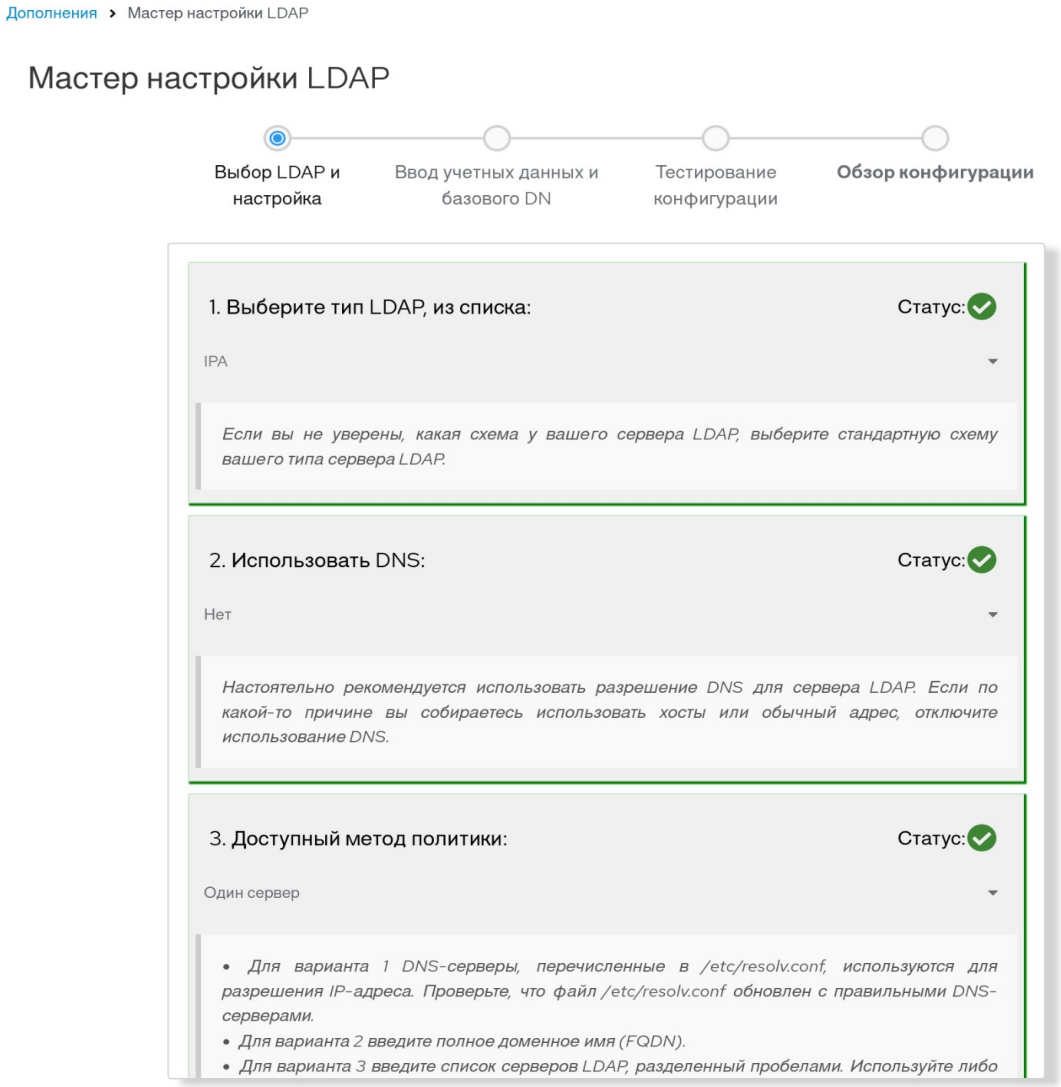

Рисунок 95 – Выбор типа LDAP сервера, использования DNS и политик использования

Далее введите IP-адрес хоста сервера IPA и используемый протокол (по умолчанию используется plain) (рисунок 96).

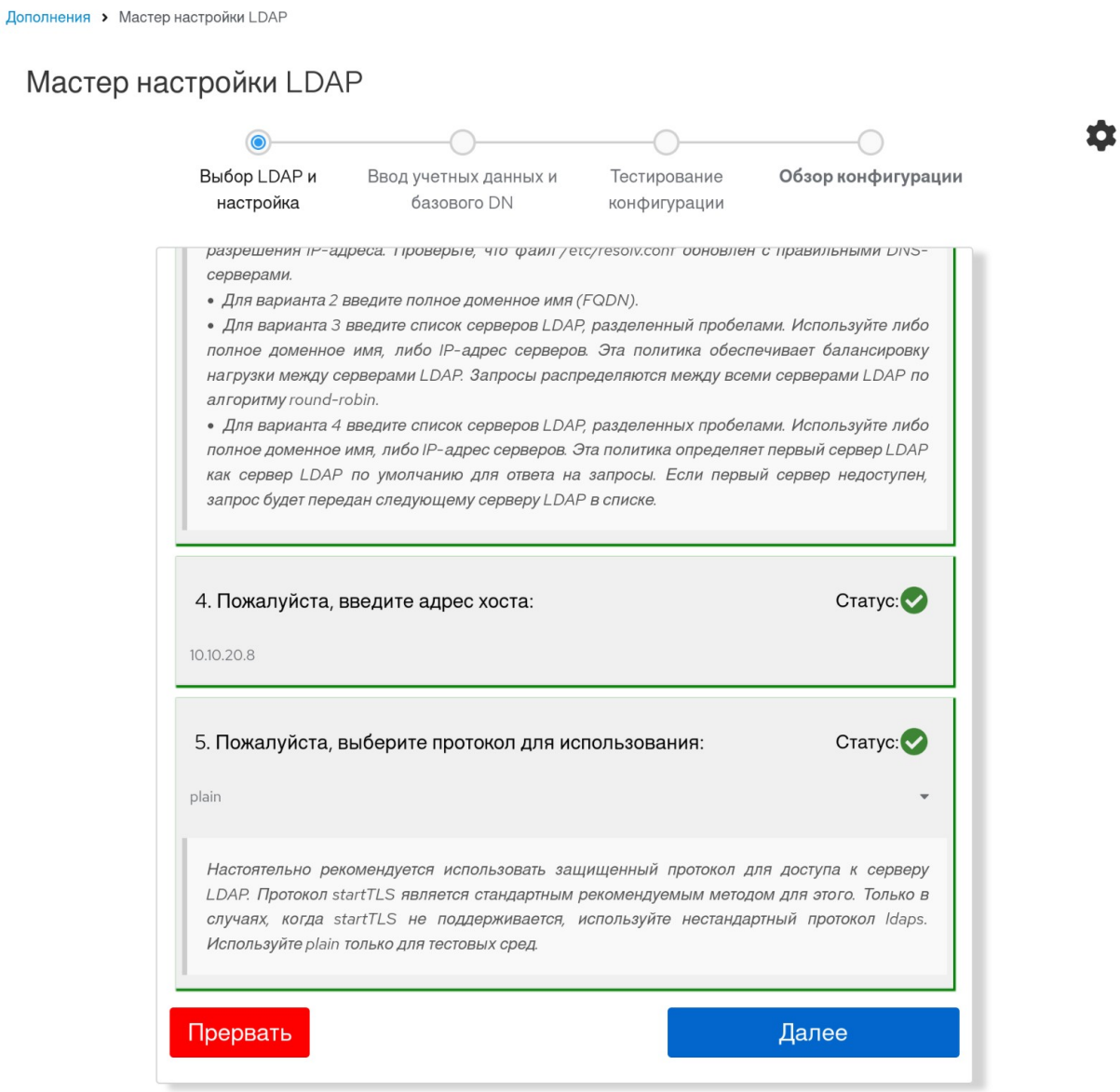

Рисунок 96 – Ввод IP-адреса хоста и типа используемого LDAP протокола

Нажмите кнопку Далее для перехода на следующий экран "Мастера настройки LDAP" (рисунок 97).

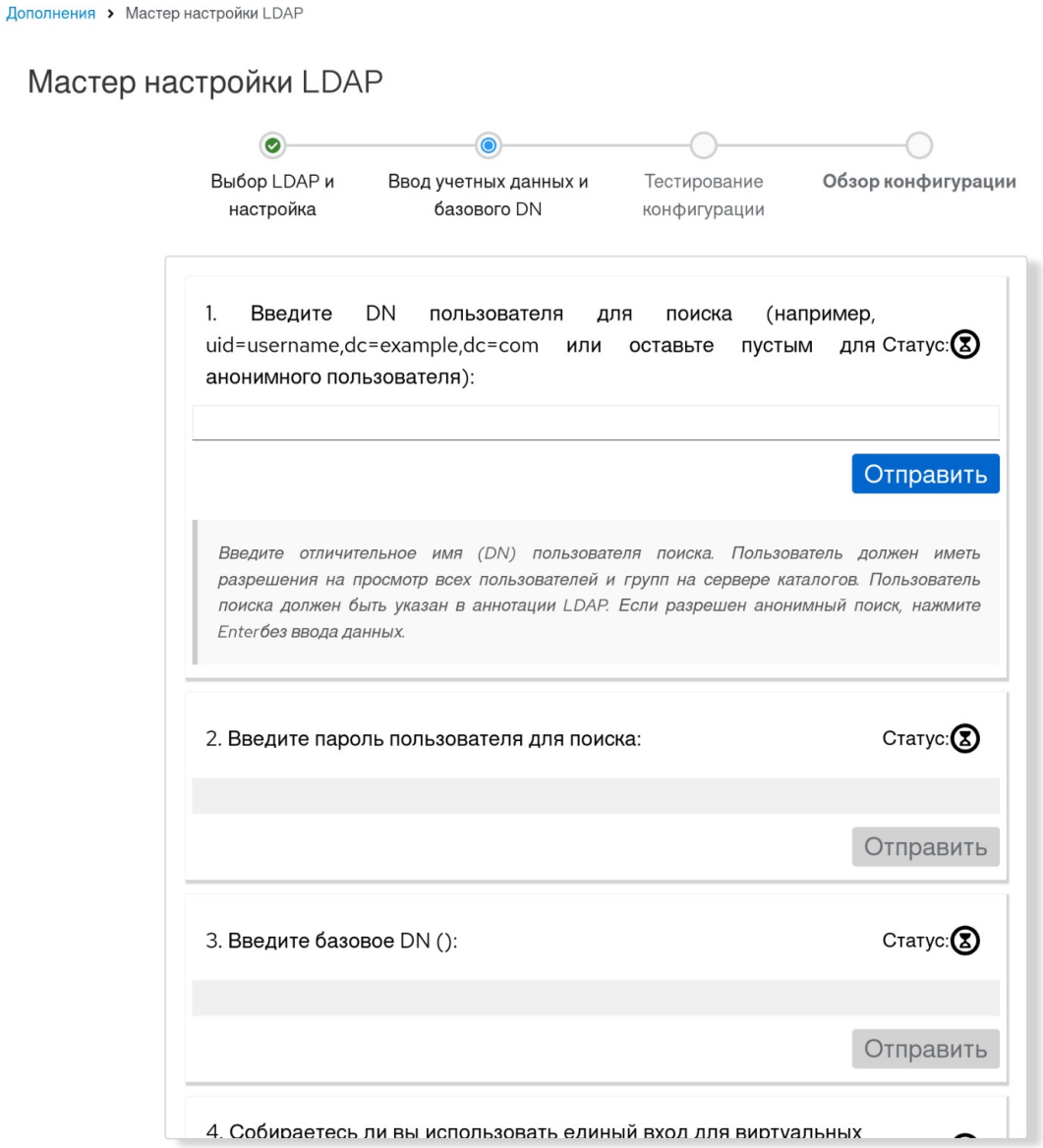

Рисунок 97 – Форма "Ввод учетных данных и базового DN" Мастера настройки LDAP

Введите DN для учетной записи susvengine, созданной ранее (рисунок 98).

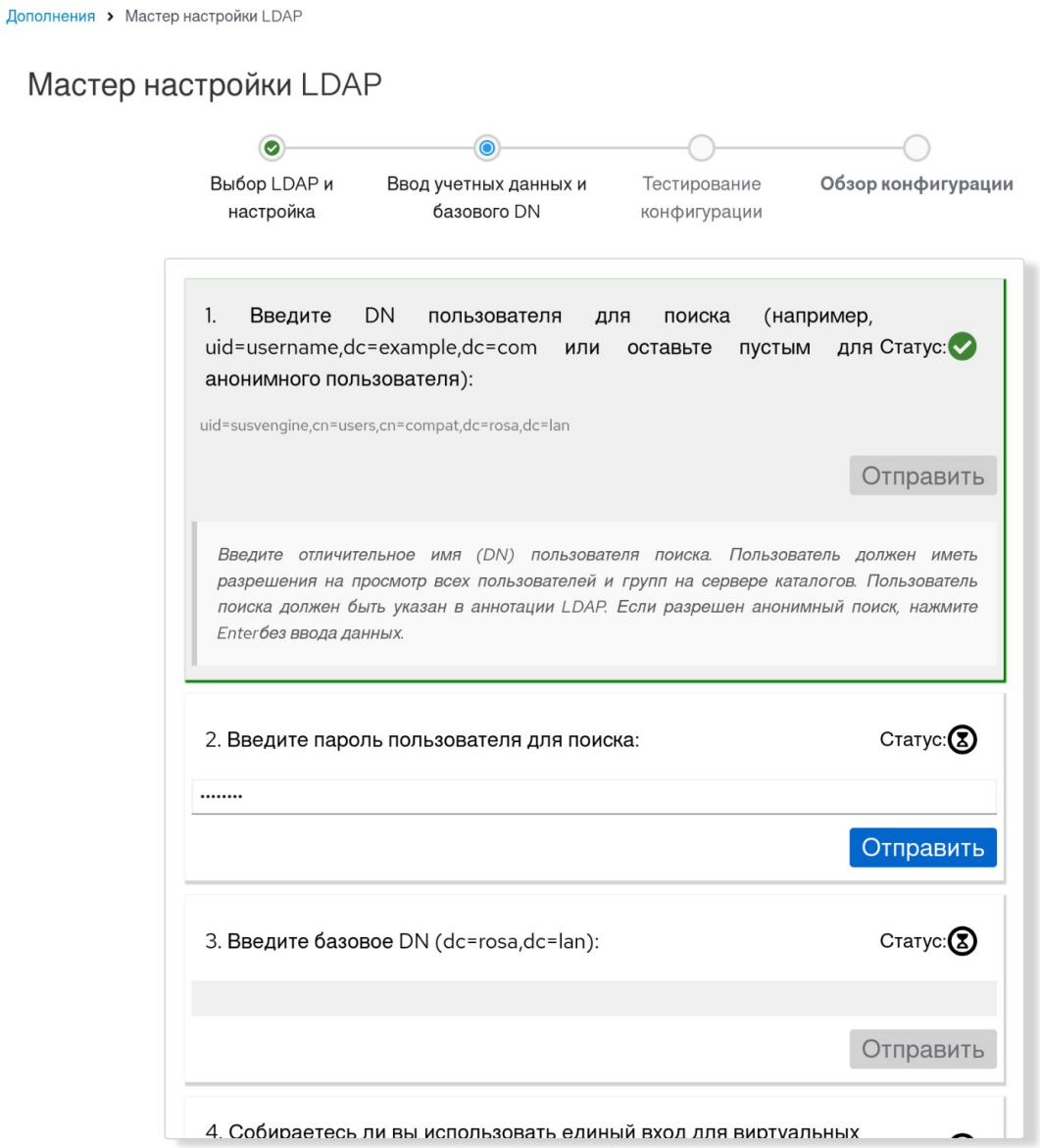

Рисунок 98 – Ввод DN сервисной учетной записи

В примере выше DN определяется как:

```
dn: uid=susvengine,cn=users,cn=compat,dc=rosa,dc=lan
```

Для получения параметров DN в вашем конкретном случае можно использовать команду `ldapsearch` в консоли сервера IPA:

```
# ldapsearch -x uid=susvengine | grep dn
dn: uid=susvengine,cn=users,cn=compat,dc=rosa,dc=lan
dn: uid=susvengine,cn=users,cn=accounts,dc=rosa,dc=lan
```

Для интеграции с СУСВ надо использовать первое значение DN (которое включает "cn=compat").

В секции 2 введите пароль сервисной учетной записи, а в секции 3 – параметры настроенного домена (в примере – "dc=rosa,dc=lan") (рисунок 99).

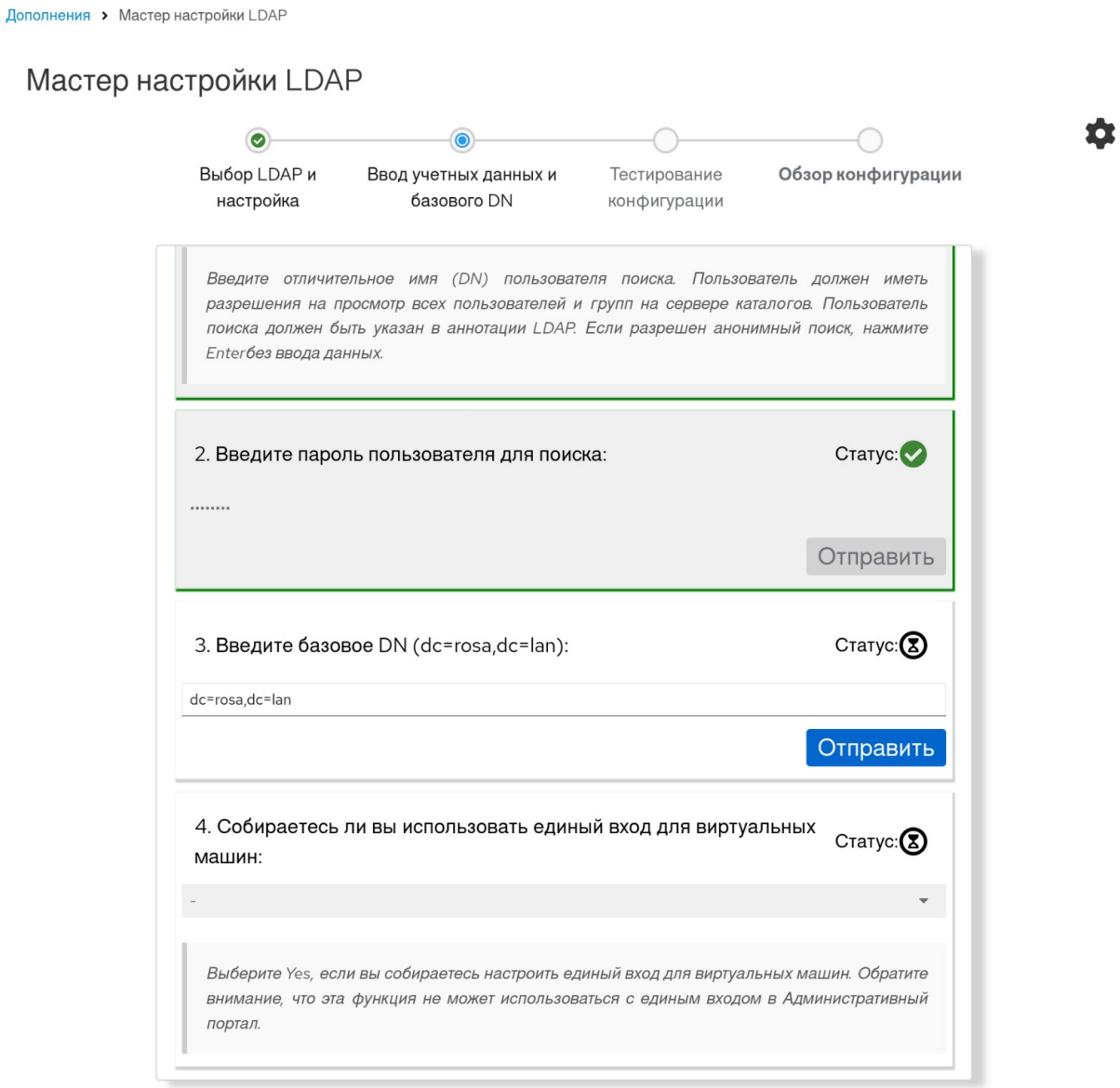

Рисунок 99 – Ввод пароля сервисной учетной записи и параметров домена

В пункте 4 введите "Да", в пункте 5 укажите имя профиля сервера LDAP, который будет виден пользователям при входе на Портал администрирования или Портал виртуальных машин, например "RV" (рисунок 100).

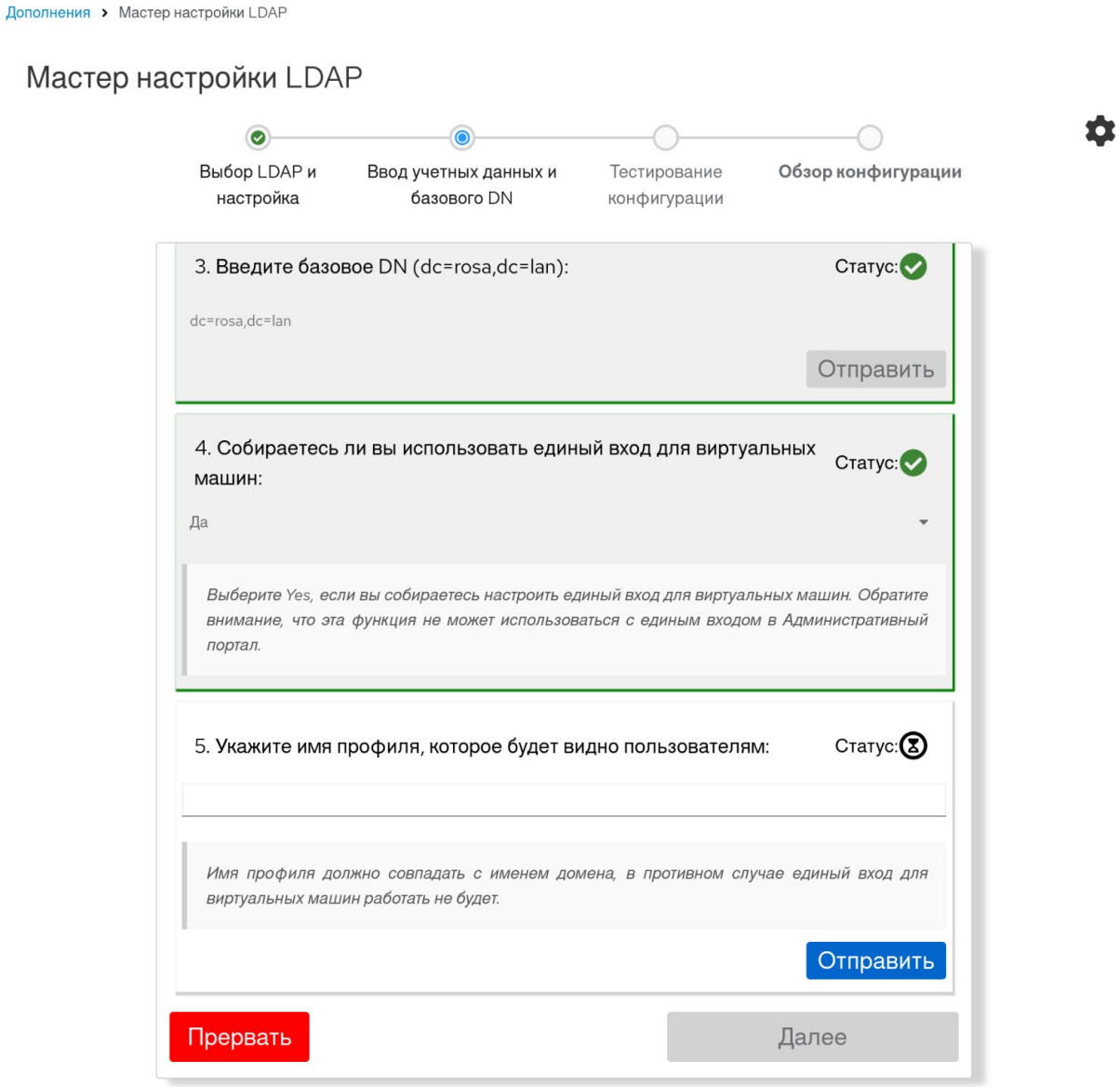

Рисунок 100 – Настройка единого входа и имени профиля сервера LDAP

Затем нажмите на кнопку Далее для перехода в форму "Тестирование и конфигурации" (рисунок 101).

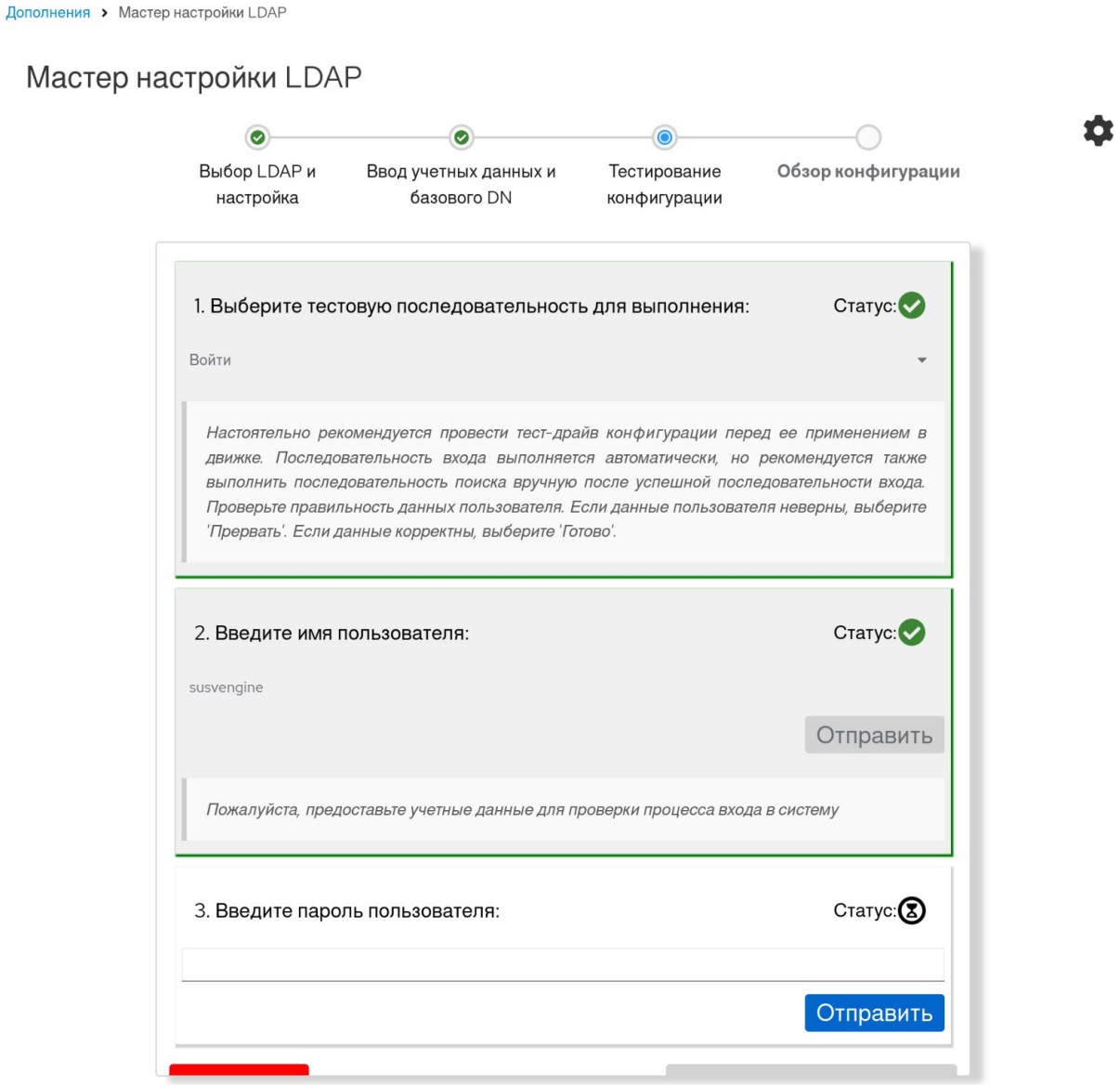

Рисунок 101 – Тестирование конфигурации LDAP

В форме тестирования конфигурации введите тестовую последовательность для выполнения (секция 1) – "Войти", имя пользователя сервисной учетной записи (в примере – "susvengine") и пароль пользователя (рисунок101).

Далее нажмите на кнопку Отправить.

Если все действия были выполнены корректно и "логин/пароль" соответствуют, то на экране появится подтверждение успешности выполненного входа (рисунок 102).

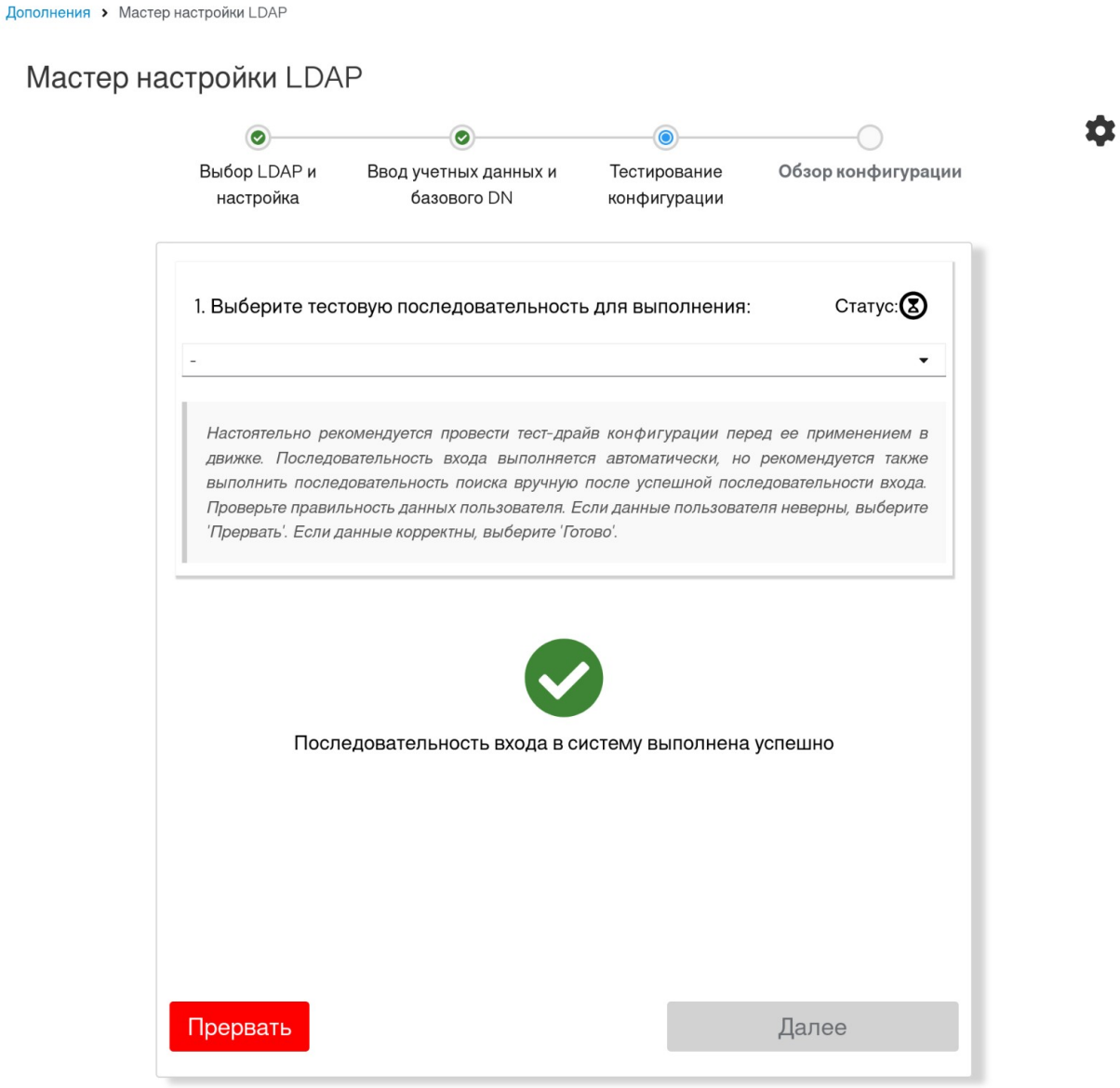

Рисунок 102 – Вход выполнен успешно

Выберите в секции 1 последовательность для выполнения "Готово" и нажмите на кнопку Далее (рисунок 103).

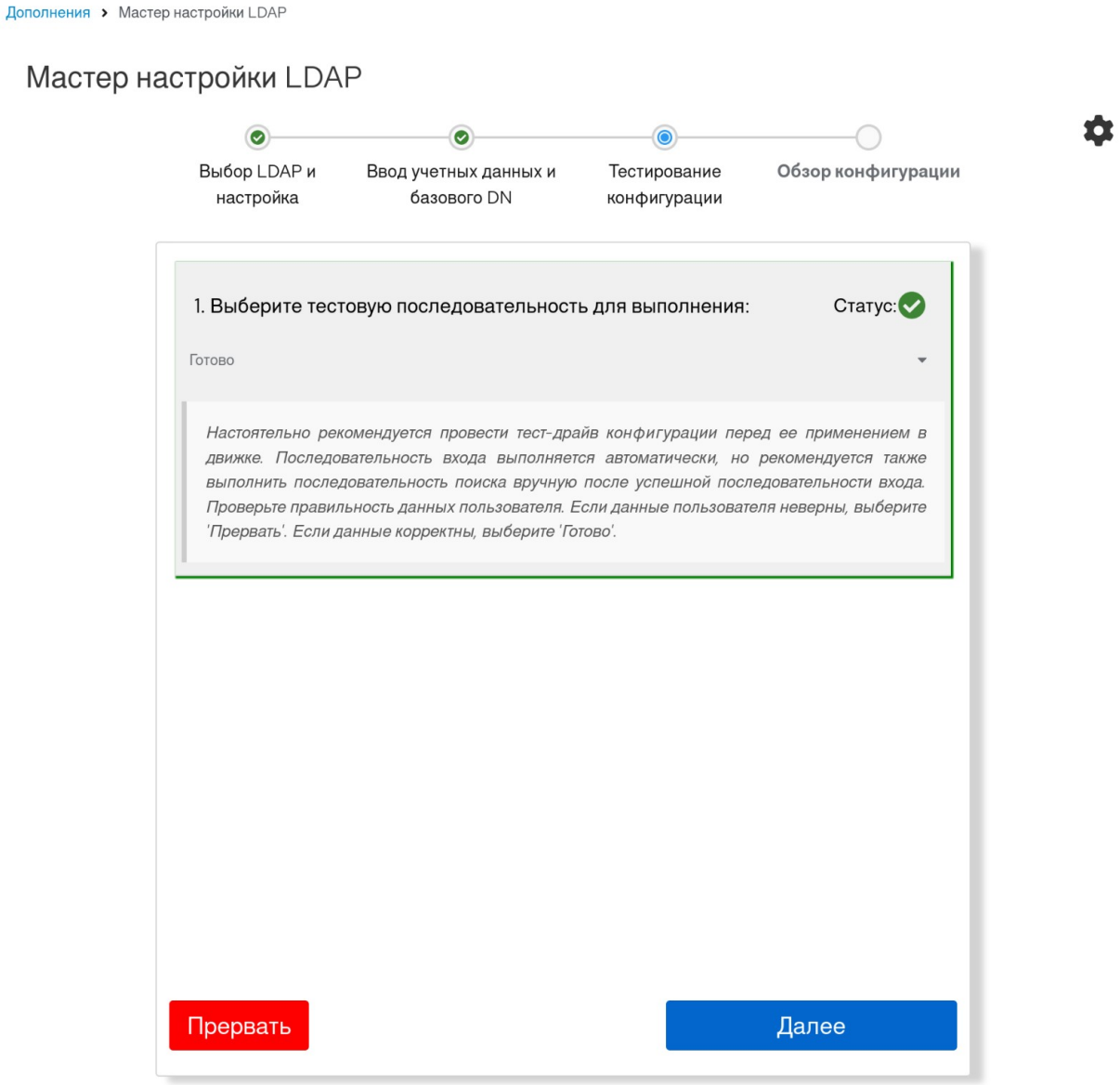

Рисунок 103 – Завершение тестирования конфигурации LDAP

На последнем экране "Мастера настройки LDAP" отображается настроенная конфигурация.

Нажмите на кнопку Завершить для завершения настройки конфигурации LDAP (рисунок 104).

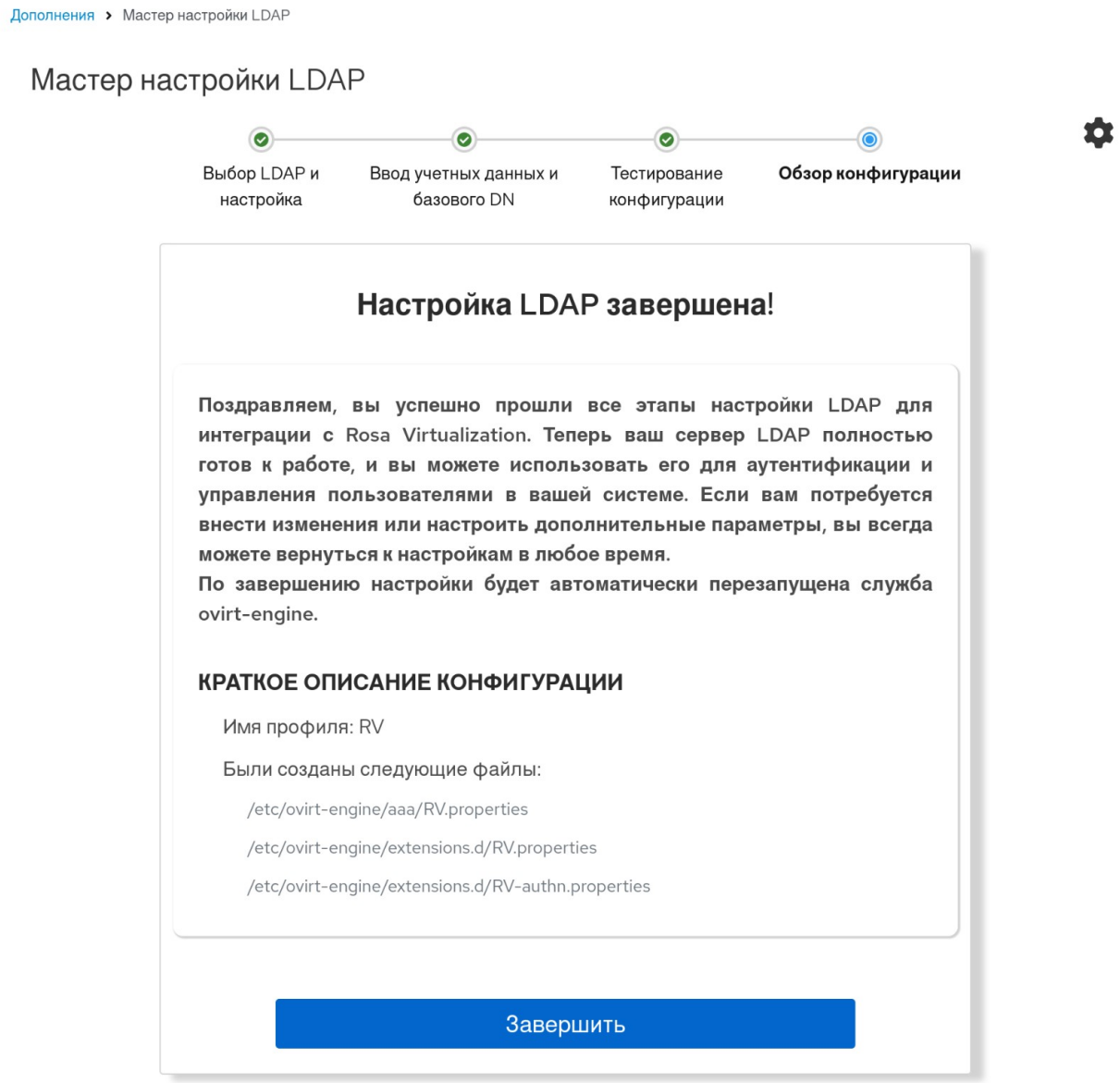

Рисунок 104 – Обзор конфигурации настройки интеграции с LDAP сервером

3.9.3 Создание профиля подключения к службе каталогов LDAP сервера IPA с помощью командной строки

Настройка подключения ROSA Virtualization к службе каталогов LDAP сервера IPA с помощью командной строки осуществляется утилитой ovirt-engine-extension-aaa-ldap-setup в консоли СУСВ.

Примечание – Если вы уже настроили интеграцию с LDAP сервером с помощью веб-интерфейса и "Мастера настройки LDAP", то данную секцию вы можете пропустить.

Для подключения к консоли СУСВ по SSH выполните следующую команду с указанием доменного имени (например, "ipa.rosa.lan") или IP-адреса ВМ СУСВ,

а также пароля учетной записи суперпользователя root ВМ СУСВ при выводе на экран соответствующего запроса:

```
$ ssh root@ipa.rosa.lan
(root@ipa.rosa.lan) Password:
```

3.9.3.1 Запуск интерактивного сценария настройки подключения ROSA Virtualization к службе каталогов LDAP

Для запуска интерактивного сценария настройки и создания профиля подключения с целью идентификации и аутентификации доменных пользователей выполните в консоли СУСВ следующую команду:

```
# ovirt-engine-extension-aaa-ldap-setup
```

Сценарий настройки предложит выбрать тип реализации сервера LDAP из пронумерованного списка. Для выбора **сервера IPA** введите цифру "6":

```
Available LDAP implementations:
 1 - 389ds
 2 - 389ds RFC-2307 Schema
 3 - Active Directory
 4 - IBM Security Directory Server
 5 - IBM Security Directory Server RFC-2307 Schema
 6 - IPA
 7 - Novell eDirectory RFC-2307 Schema
 8 - OpenLDAP RFC-2307 Schema
 9 - OpenLDAP Standard Schema
10 - Oracle Unified Directory RFC-2307 Schema
11 - RFC-2307 Schema (Generic)
12 - RHDS
13 - RHDS RFC-2307 Schema
14 - iPlanet
Please select: 6
```

Далее сценарий настройки предложит использовать разрешение имени DNS для сервера IPA:

– Если в сети используется сервер DNS, нажмите клавишу `Enter` или введите "Yes".

– При отсутствии в сети сервера DNS введите "No":

```
Use DNS (Yes, No) [Yes]: No
```

Примечание – При отсутствии в сети сервера DNS доменные имена и IP-адреса хостов, СУСВ и сервера IPA должны быть указаны в файле /etc/hosts сервера IPA, а также на хостах ROSA Virtualization и СУСВ. Отредактируйте файл /etc/hosts на каждом из перечисленных выше хостов и серверов, указав актуальные доменные имена и IP-адреса.

Из пронумерованного списка выберите метод реализации политики службы DNS. При выборе варианта 1 (Single server) введите IP-адрес сервера IPA:

```
    Available policy method:
    1 - Single server
    2 - DNS domain LDAP SRV record
    3 - Round-robin between multiple hosts
    4 - Failover between multiple hosts
    Please select: 1
    Please enter host address: 10.10.20.8
```

Примечание – Указанный в выводе консоли выше IP-адрес "10.10.20.8" является примером, необходимо указать IP-адрес, соответствующий серверу IPA, установленному в вашем ЦОД.

Далее сценарий настройки предложит выбрать протокол подключения к каталогу LDAP, а также указать отличительное имя и пароль пользователя для выполнения запросов поиска в каталоге LDAP. Введите значение "plain" для выбора протокола и следующие атрибуты ранее созданной служебной записи пользователя:

```
    Please select protocol to use (startTLS, ldaps, plain)
[startTLS]:
    plain
    Enter search user DN (for example
uid=username,dc=example,dc=com or leave empty for anonymous):
    uid=susvengine,cn=users,cn=compat,dc=rosa,dc=lan
    Enter search user password:
```

Примечание – Пример выше предполагает, что на сервере IPA, управляющим доменом rosa.lan, была создана служебная учетная запись susvengine с отличительным именем (dn) – "uid=susvengine,cn=users,cn=compat,dc=rosa,dc=lan".

Отличительное имя (уникальное имя) dn – это имя, уникальным образом идентифицирующее каждую запись каталога LDAP. При вводе параметров в сценарий установки используйте отличительное имя служебной учетной записи,

созданной ранее на сервере IPA для выполнения синхронизации с ROSA Virtualization.

Для проверки корректности указанного отличительного имени dn используйте на сервере IPA в командной строке следующую команду:

```
# ipa user-show engine --all --raw | grep dn:
  dn: uid=susvengine,cn=users,cn=accounts,dc=rosa,dc=lan
```

Далее сценарий настройки предложит определенные значения по умолчанию для следующих параметров:

```
Please enter base DN (dc=rosa,dc=lan) [dc=rosa,dc=lan]:
Are you going to use Single Sign-On for Virtual Machines
(Yes, No) [Yes]:
```

Чтобы принять предложенные значения по умолчанию, нажмите клавишу `Enter`.

Сценарий настройки предложит указать имя для профиля подключения. Введите наименование профиля (например, "RV"):

```
Please specify profile name that will be visible to users:
RV
```

Примечание – Данный профиль будет использоваться для входа в Портал администрирования и Портал ВМ ROSA Virtualization (рисунок 105).

Для тестовой проверки подключения укажите имя и пароль ранее созданной служебной записи пользователя (в примере ниже учетная запись имеет имя "susvengine"):

```
Please provide credentials to test login flow
Enter user name: susvengine
Enter user password:
```

Сценарий настройки приступит к созданию профиля подключения в соответствии с заданной конфигурацией.

3.9.3.2 Перезагрузка службы ovirt-engine

После завершения процедуры создания профиля выполните перезагрузку службы ovirt-engine:

```
# systemctl restart ovirt-engine
```

В результате созданный профиль подключения RV станет доступен для выбора в окне авторизации при входе на Портал администрирования СУСВ (рисунок 105) или на Портал ВМ.

3.9.4 Вход в портал администрирования и портал ВМ с использованием логина и пароля корпоративного LDAP сервера

Откройте в новом окне браузера форму входа на Портал администрирования или Портал виртуальных машин и выберите Портал администрирования (для учетной записи администратора) или Портал виртуальных машин (для учетной записи пользователя).

В выпадающем меню "Профиль" выберите домен авторизации, настроенный при конфигурировании доступа к серверу LDAP. В полях "Имя пользователя" и "Пароль" укажите логин и пароль учетной записи пользователя, настроенной в корпоративном LDAP-сервере (контроллере домена). Далее нажмите на копку Вход в систему (рисунок 105). При наличии у пользователя соответствующих прав будет осуществлен вход в портал.

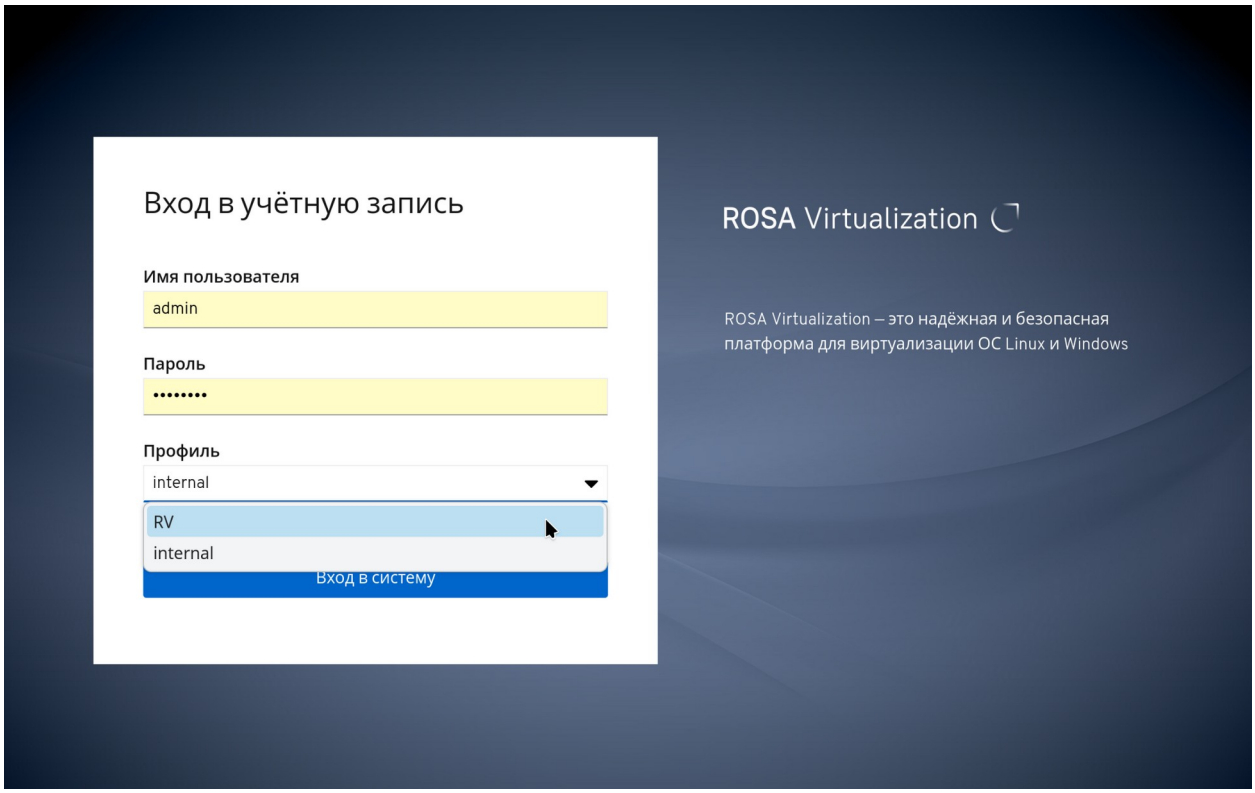

Рисунок 105 – Выбор профиля подключения RV в окне авторизации при входе на портал администрирования СУСВ

3.9.4.1 Предоставление прав доступа к ресурсам ROSA Virtualization для пользователей сервера IPA

Назначение необходимых прав доступа к ресурсам ROSA Virtualization для новых созданных пользователей сервера IPA осуществляется на Портале администрирования СУСВ.

Для доступа к списку пользователей выберите пункт "Администрирование → Пользователи" в главном меню СУСВ (рисунок 106).

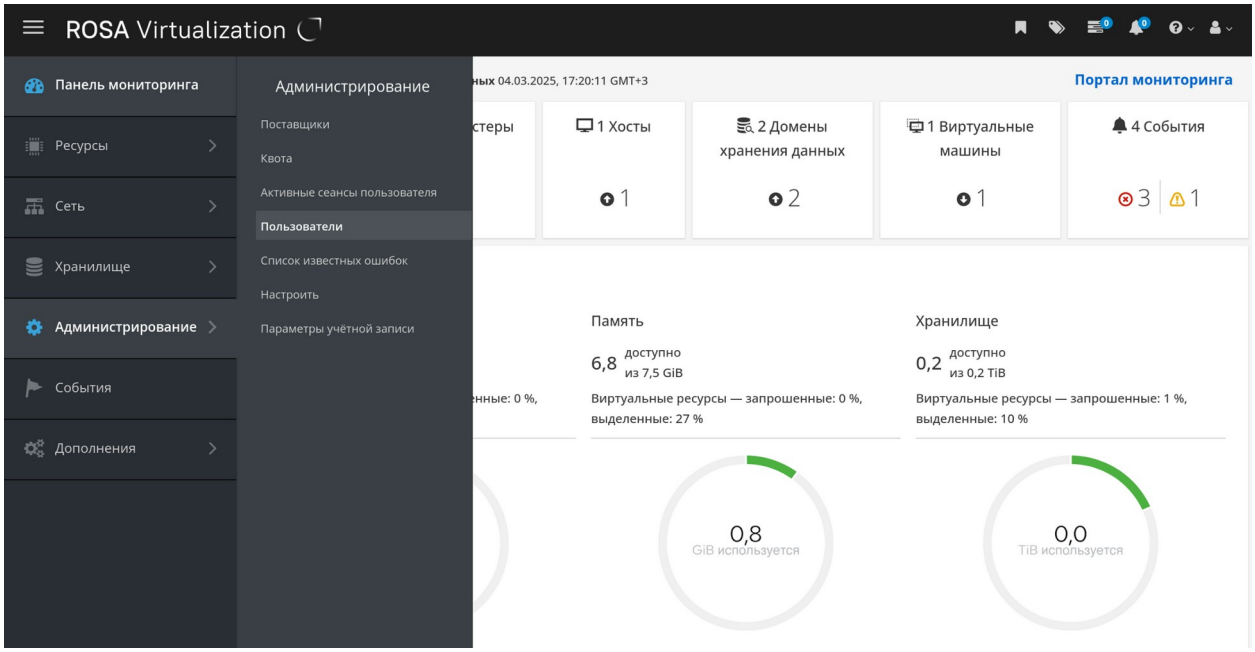

Рисунок 106 – Раздел в главном меню панели администрирования СУСВ

На странице "Администрирование → Пользователи" отображается список пользователей, авторизованных для работы с Платформой виртуализации ROSA Virtualization (рисунок 107).

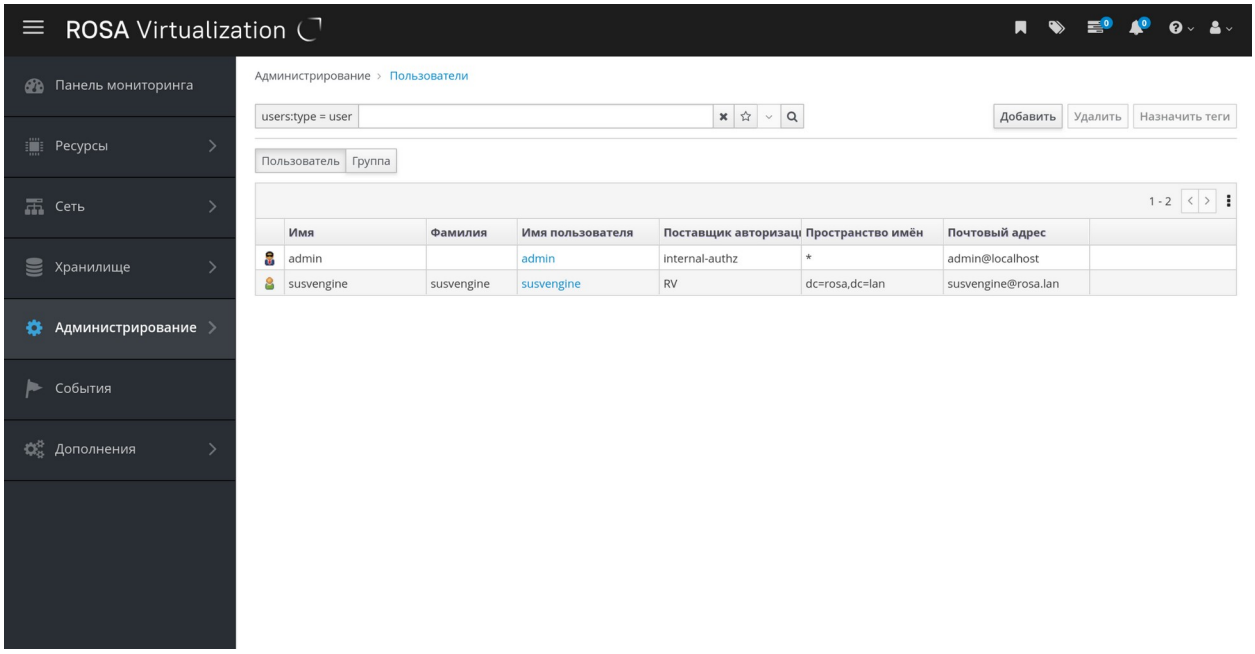

Рисунок 107 – Список пользователей, авторизованных для работы с Платформой виртуализации ROSA Virtualization

Для добавления пользователя нажмите на кнопку Добавить.

Введите в форму логин пользователя, принадлежащего пространству имён присоединенного домена, и нажмите на кнопку Вперед (рисунок 108).

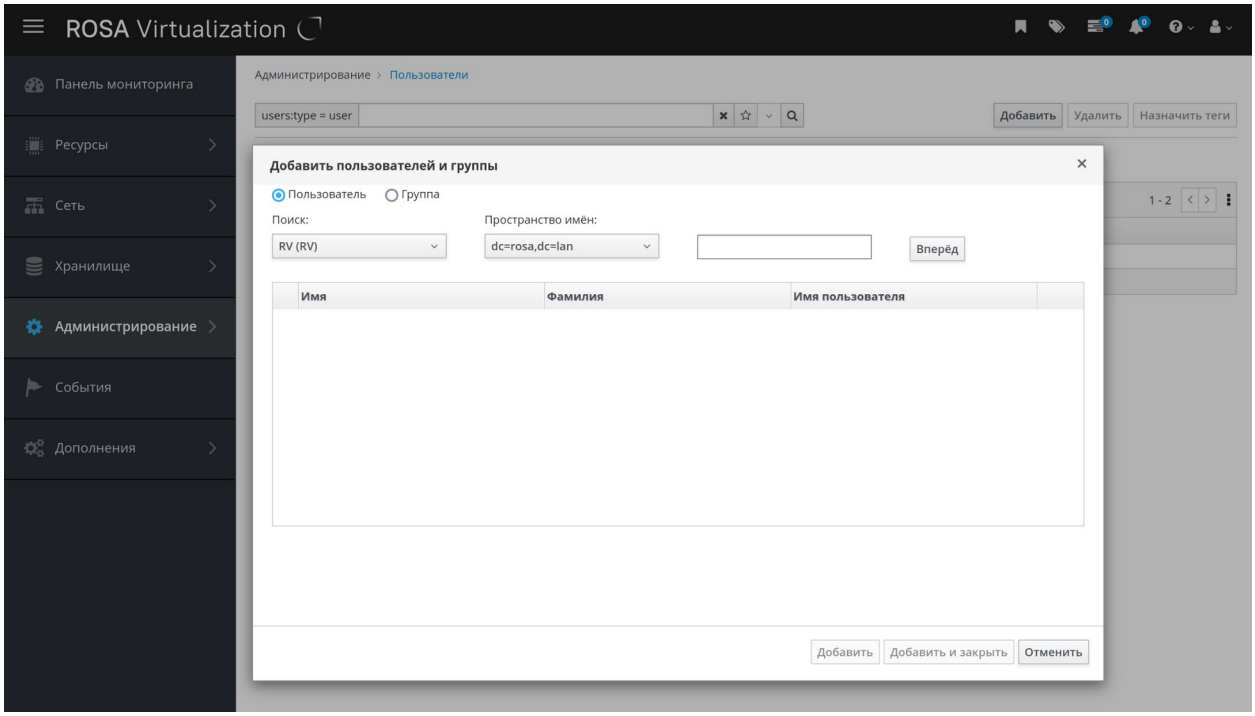

Рисунок 108 – Добавление пользователя из корпоративного каталога LDAP

Выберите необходимого пользователя и нажмите на кнопку Добавить и закрыть (рисунок 109).

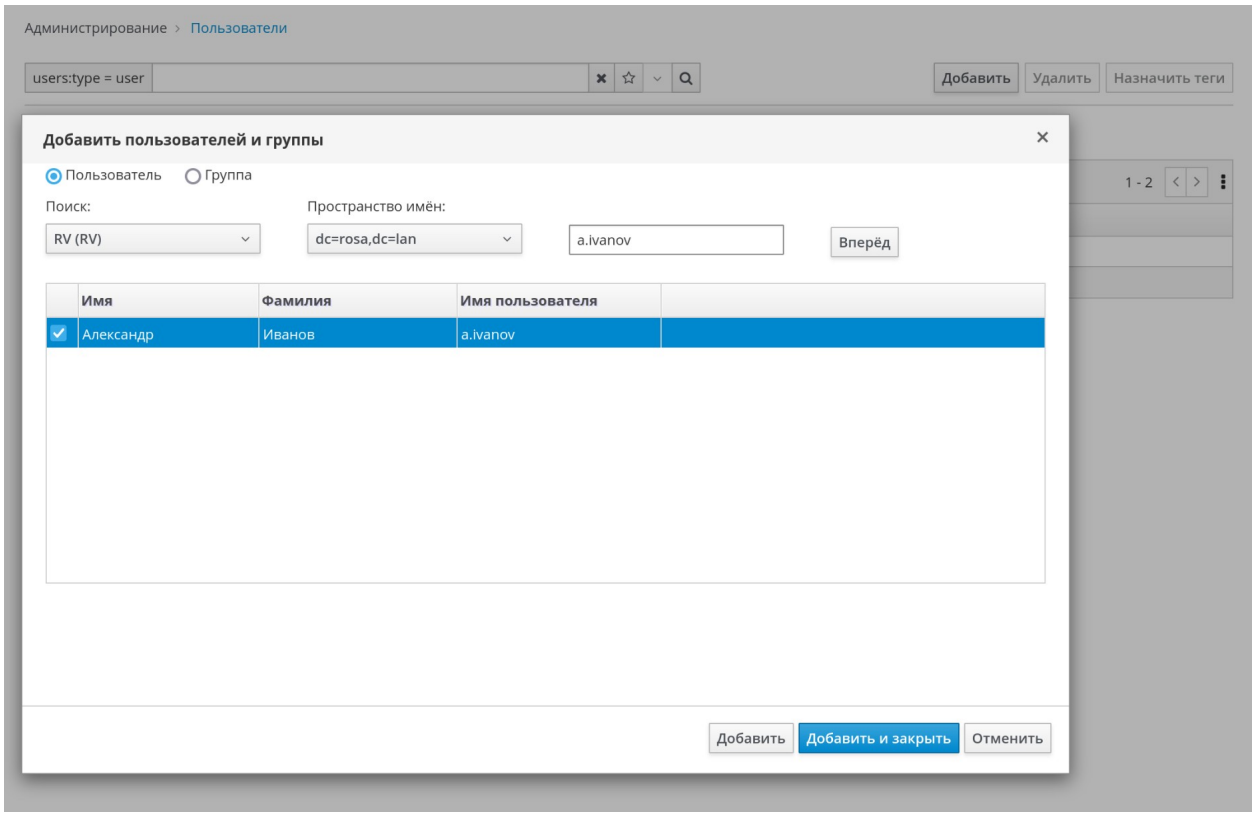

Рисунок 109 – Поиск пользователя домена по логину

Пользователь будет добавлен к списку пользователей, авторизованных для работы с Платформой ROSA Virtualization (рисунок 110).

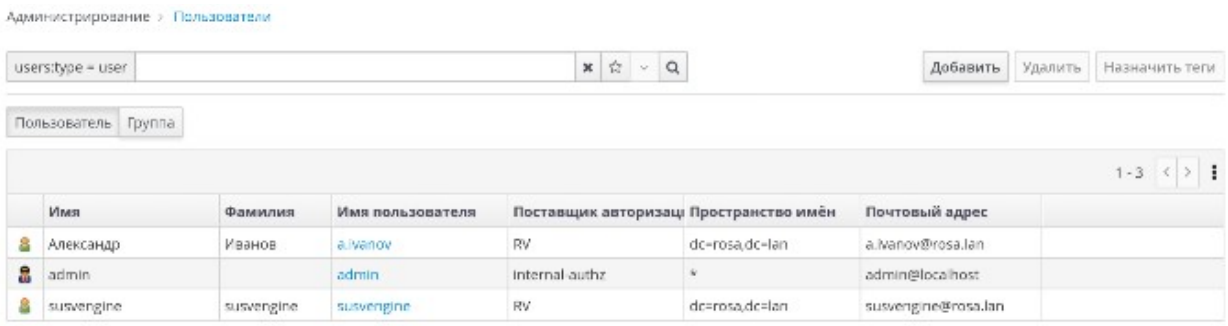

Рисунок 110 – Обновленный список пользователей Платформы

Далее необходимо предоставить пользователю права на доступ к конкретным ресурсам.

Для предоставления прав доступа нажмите на логин пользователя в списке (рисунок 110). Откроется форма с информацией о данном пользователе (рисунок 111).

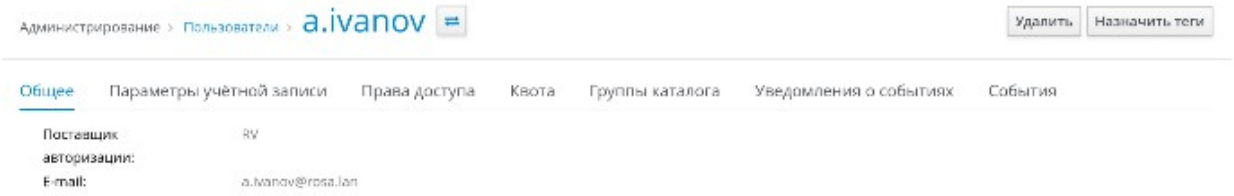

Рисунок 111 – Информация о пользователе a.ivanov

Перейдите на вкладку "Права доступа".

Нажмите на кнопку `Добавить системные полномочия` (рисунок 112).

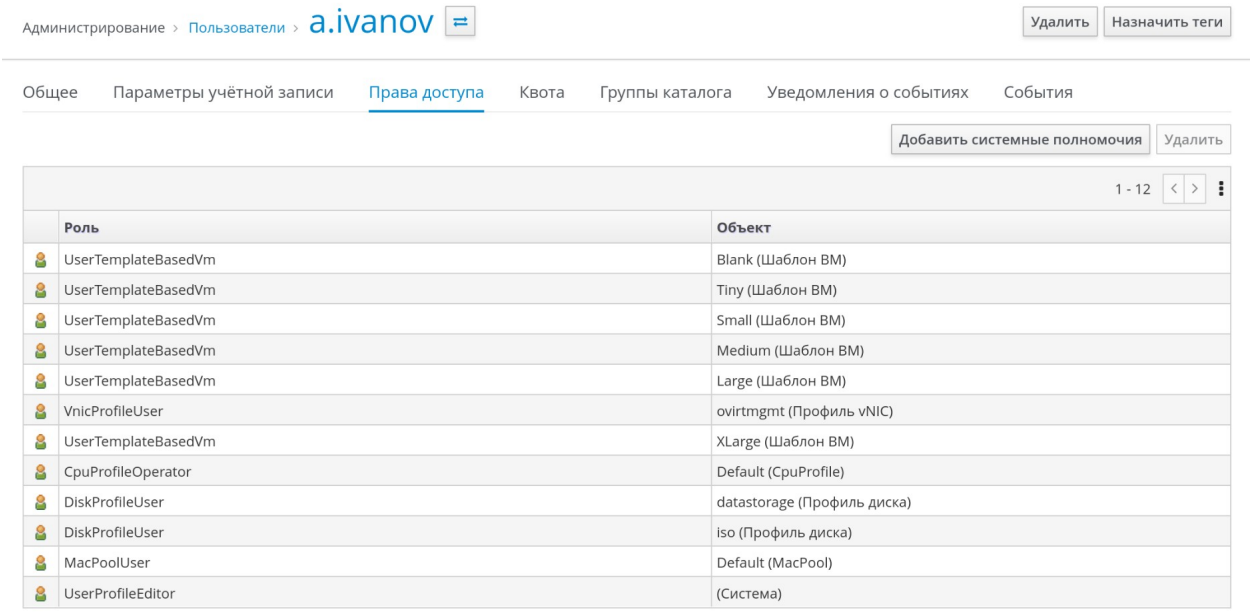

Рисунок 112 – Права доступа пользователя

Выберите требуемые полномочия, например для опытного пользователя можно выбрать "PowerUserRole" (пользователь с расширенными полномочиями) (рисунок 113).

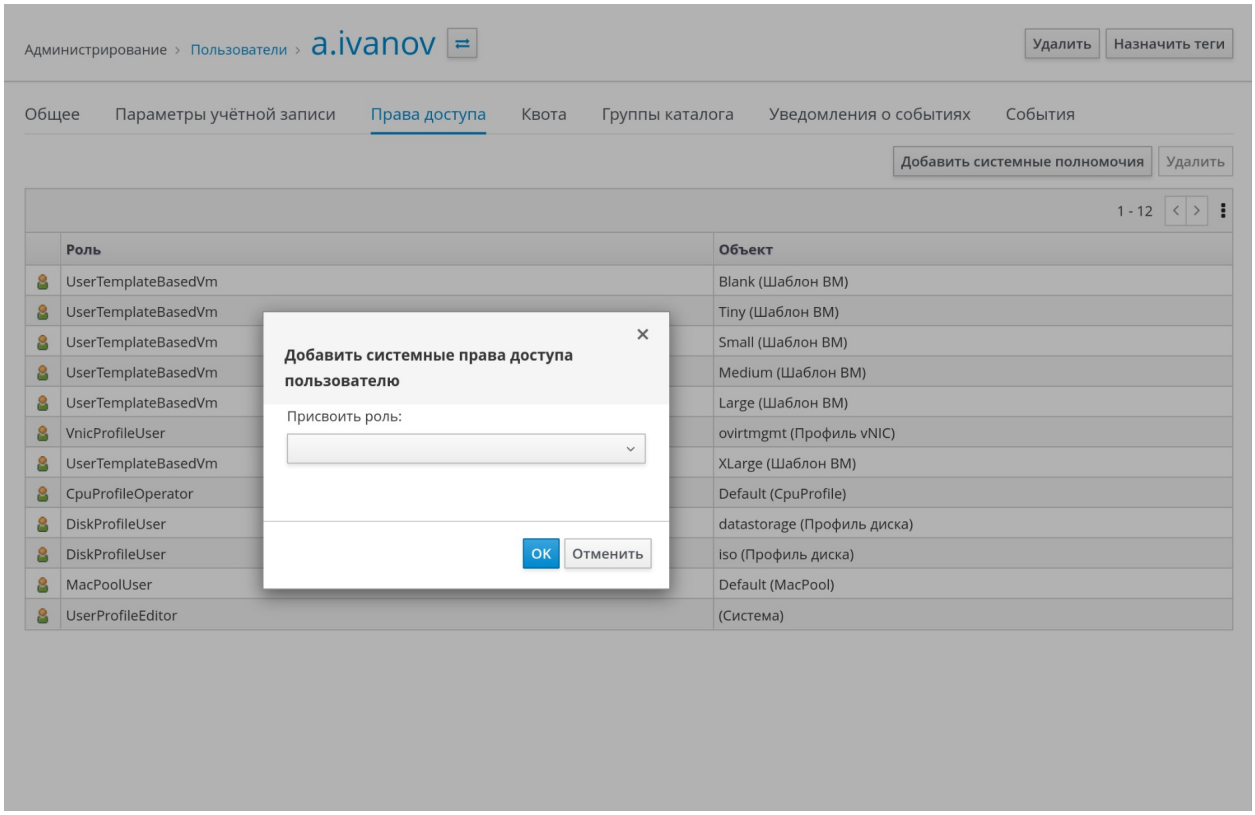

Рисунок 113 – Добавление системных полномочий

Присвоение роли "PowerUserRole" осуществляется во вкладке "Права доступа" (рисунок 114).

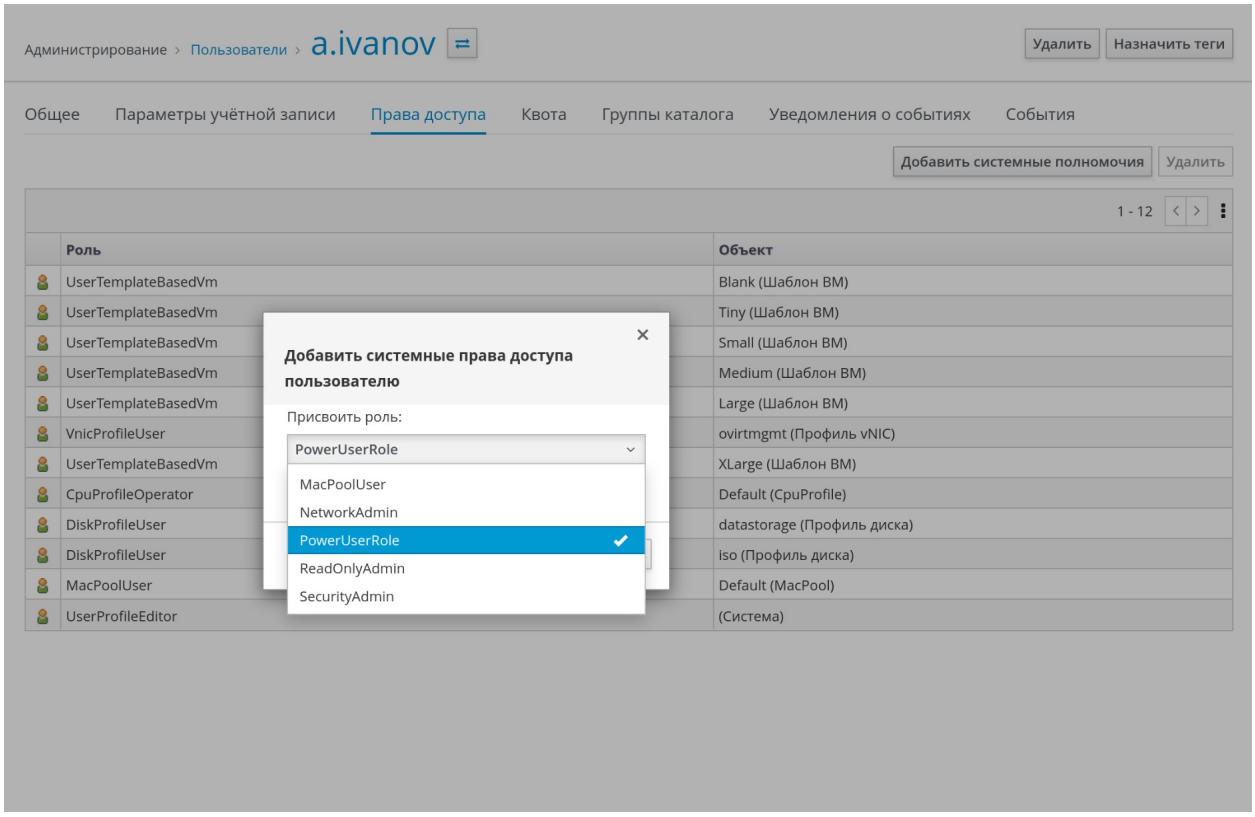

Рисунок 114 – Добавление системных прав пользователю

После выбора необходимых прав нажмите на кнопку `OK` для добавления указанных прав и полномочий (рисунок 115).

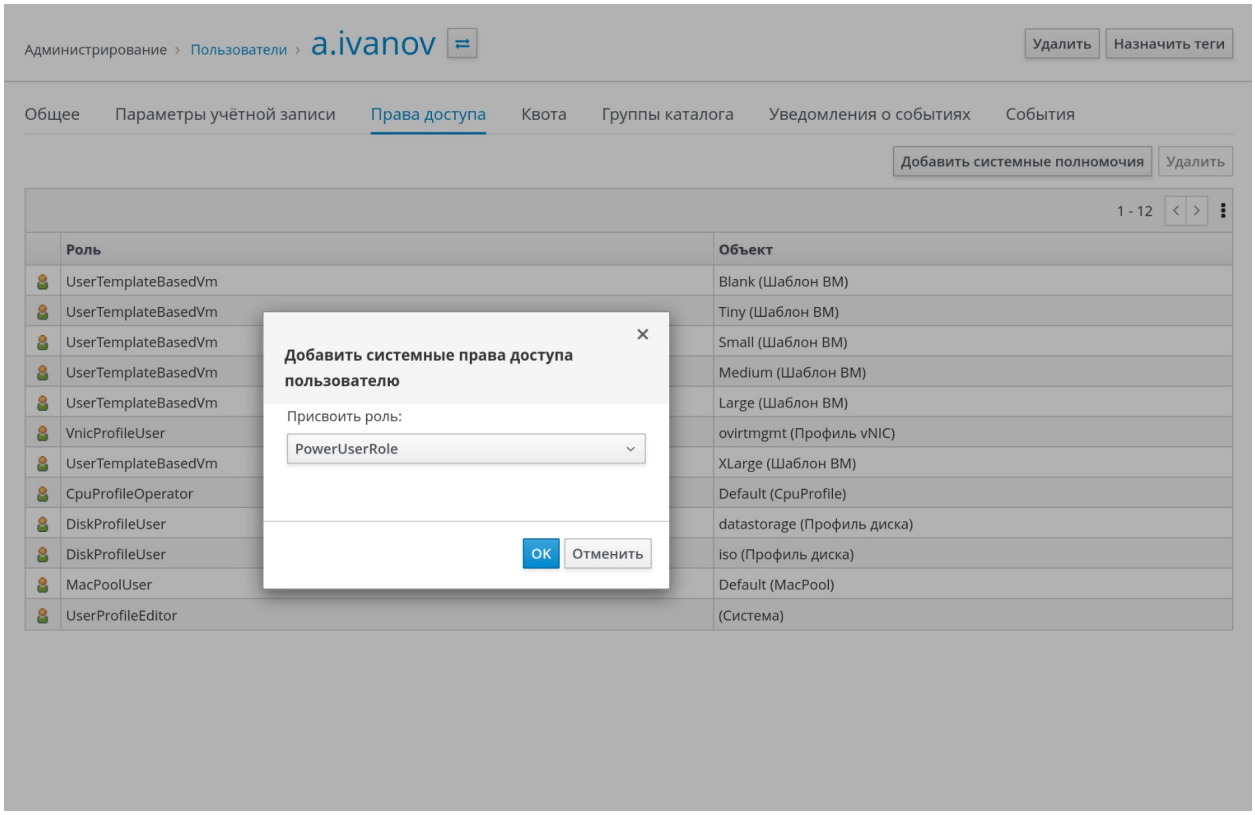

Рисунок 115 – Добавление выбранных прав пользователю

Выбранные права появятся в списке прав пользователя (рисунок 116).

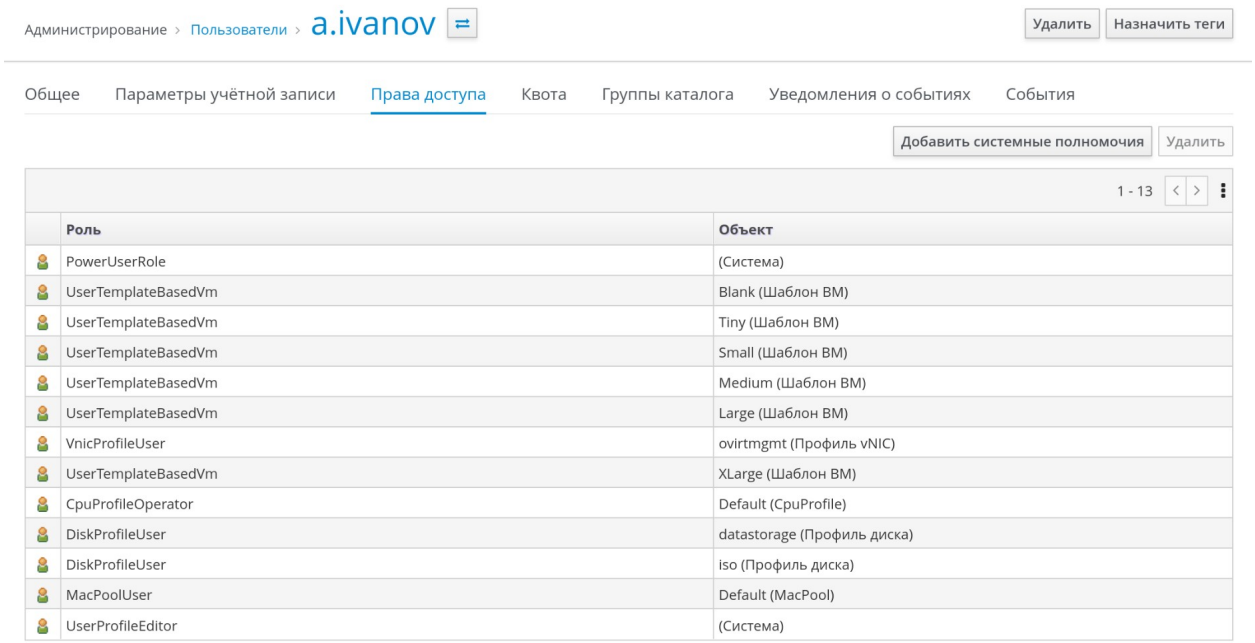

Рисунок 116 – Обновленный список прав пользователя

Войдите с помощью аккаунта пользователя, которому были выше добавлены права, в Портал ВМ.

Вход будет успешно осуществлен, и пользователь увидит интерфейс Портала ВМ для запуска и создания ВМ (рисунок 117).

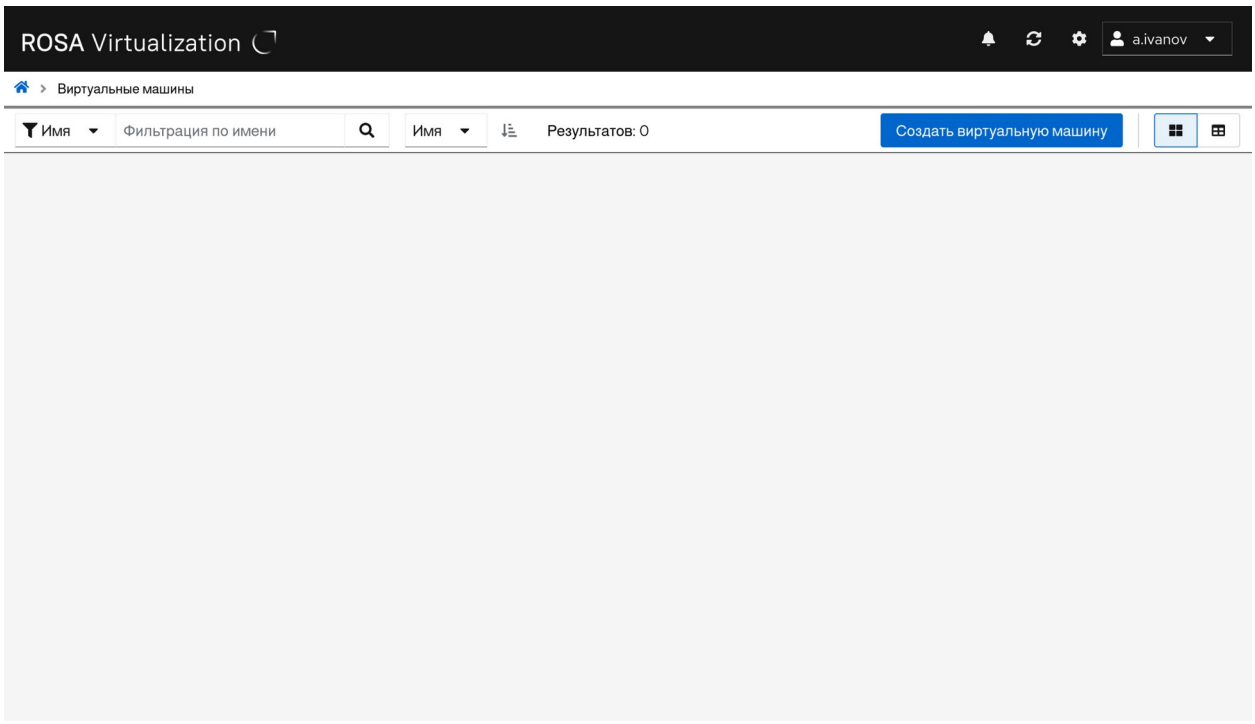

Рисунок 117 – Интерфейс Портала ВМ, доступный пользователю с правами "PowerUser"

Нажмите на кнопку `Создать виртуальную машину` (рисунок 117).

Откроется интерфейс для создания ВМ (доступно пользователю с ролью "PowerUser") (рисунок 118).

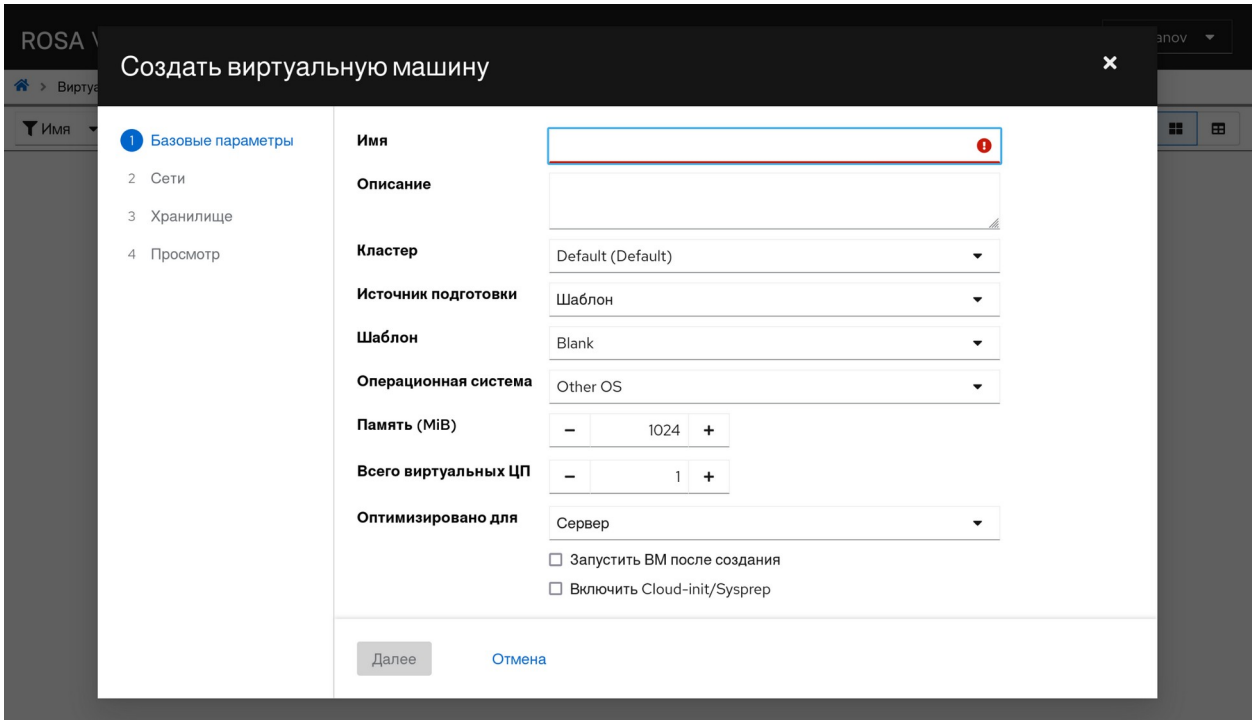

Рисунок 118 – Интерфейс создания ВМ для пользователя с ролью "PowerUser"

При необходимости повторите операцию по добавлению пользователей и наделению их правами для других пользователей, зарегистрированных на корпоративном LDAP сервере.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Определение
ВМ	Виртуальная машина
ВЦОД	Виртуальный центр обработки данных
ГОСТ	Государственный стандарт
МСЭ	Международный союз электросвязи
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПО	Программное обеспечение
СУБД	Система управления базами данных
СУСВ	Система управления средой виртуализации
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ЦОД	Центр обработки данных
ЦП	Центральный процессор
ЦУ	Центр управления
Ansible	Система управления конфигурациями; используется для автоматизации настройки и развёртывания программного обеспечения
API	Application Programming Interface – программный интерфейс
BIOS	Basic input / output system – базовая система ввода / вывода
CA	Certification authority – центр сертификации (удостоверяющий центр)
Ceph	Программно-определяемая платформа хранения данных, которая предоставляет объектное хранилище, блочное хранилище и файловое хранилище, построенное на общей распределенной кластерной основе.
CPU	Central processing unit – центральный процессор
DHCP	Dynamic host configuration protocol – протокол динамической настройки узла
DN	Distinguished Name – имя, уникальным образом идентифицирующее каждую запись каталога LDAP
DNS	Domain name system – система доменных имен
DVD	Digital versatile disc – цифровой многоцелевой диск
Ext3	Журналируемая файловая система

Сокращение	Определение
Ext4	Журналируемая файловая система
FAT	File allocation table – таблица размещения файлов
FC	Протокол Fibre Channel
FCoE	Fibre channel over Ethernet – протокол Fibre Channel, работающий поверх Ethernet
FQDN	Fully qualified domain name – полное доменное имя
GlusterFS	Распределённая, параллельная, линейно масштабируемая файловая система с возможностью защиты от сбоев
GPT	GUID partition table – формат размещения таблиц разделов на диске
GRUB	Grand unified bootloader – унифицированный загрузчик операционной системы
HDD	Hard Disk Drive – жёсткий диск
HTTP	Hypertext Transfer Protocol – протокол уровня приложений для распределённых, гипермедийных информационных систем
HTTPS	Hyper Text Transfer Protocol Secure – расширение протокола HTTP для поддержки шифрования в целях повышения безопасности
ID	Identification Data – идентификатор
IDE	Integrated Drive Electronics – интерфейс подключения накопителей к компьютеру
IP	Internet protocol – протокол межсетевого взаимодействия
IPA	Identity, policy and audit – система идентификации и аутентификации пользователей, задания политик доступа и аудита
iSCSI	Internet small computer system interface – версия протокола SCSI, базирующаяся на TCP/IP
ISO	International Organization for Standardization – международная организация, занимающаяся выпуском стандартов
ITU-T	Сектор стандартизации электросвязи МСЭ
JBOD	Just a bunch of disks – массив дисков
KSM	Kernel Shared Memory – объединение одинаковых страниц памяти ядром ОС
KVM	Kernel-based Virtual Machine – виртуальная машина на основе ядра ОС Linux

Сокращение	Определение
LDAP	Lightweight directory access protocol – протокол доступа к каталогам
LUKS	Linux unified key setup – спецификация формата шифрования дисков
LUN	Logical Unit Number – номер логического устройства
LVM	Logical volume management – менеджер логических томов
MAC	Media Access Control – уникальный идентификатор сетевого оборудования
MBR	Master boot record – главная загрузочная запись
NFS	Network file sharing – протокол сетевого доступа к файловым системам
NIC	Network Interface Controller – сетевой адаптер
NTP	Network time protocol – протокол сетевого времени
NVDIMM	Non-volatile dual inline memory module – энергонезависимый двойной встроенный модуль памяти
OpenSSL	криптографическая библиотека с открытым исходным кодом
OVN	Open Virtual Network – система поддержки абстракции виртуальной сети
OVN Northbound (NB) database	Центральный компонент в архитектуре открытой виртуальной сети (OVN), выступающий в качестве интерфейса между системой управления облаком (CMS) и логической сетью OVN
QCOW2	QEMU Copy on Write – формат образа тома программы QEMU
QEMU	Quick Emulator – эмулятор аппаратного обеспечения различных платформ
QXL	паравиртуализированное графическое устройство для QEMU/KVM, оптимизированное для удалённого доступа через протокол SPICE
RAID	Redundant array of independent disks – избыточный массив независимых дисков
REST	Representational State Transfer – архитектурный стиль взаимодействия компонентов распределённого приложения в сети
SAN	Storage area network – сеть хранения данных
SCSI	Small Computer System Interface – системный интерфейс
SELinux	Security Enhanced Linux – система контроля доступа,

Сокращение	Определение
	реализованная на уровне ядра ОС
SPICE	Simple Protocol for Independent Computing Environments – протокол удалённого доступа (простой протокол для независимых вычислительных сред)
SPM	Storage Pool Manager – диспетчер пула хранилища
SSH	Secure shell – защищенная оболочка
SSL	Secure Sockets Layer – уровень защищённых сокетов
TCP	Transmission Control Protocol – протокол управления передачей данных
TLS	Transport Layer Security – протокол безопасности транспортного уровня
UDP	User Datagram Protocol – сетевой протокол передачи данных
UEFI	Unified extensible firmware interface – унифицированный расширяемый интерфейс базового программного обеспечения
USB	Universal serial bus – универсальная последовательная шина
VFAT	Virtual file allocation table – виртуальная таблица размещения файлов
VLAN	Virtual local area network – виртуальная локальная вычислительная сеть
VNC	Virtual Network Computing – система (протокол) удалённого доступа в виртуальных сетях
VNIC	Virtual Network Interface Controller – виртуальный сетевой адаптер
X.509	стандарт ITU-T для инфраструктуры открытого ключа и инфраструктуры управления привилегиями
XFS	Высокопроизводительная 64-битная журналируемая файловая система
YAML	Yet Another Markup Language – язык разметки