АО "НТЦ ИТ РОСА"

СРЕДСТВО ВИРТУАЛИЗАЦИИ "РОСА ВИРТУАЛИЗАЦИЯ 4"

Версия 4.0

Руководство администратора

Часть1. Установка

РСЮК.10103-01 32 01

Листов 240

2026

АННОТАЦИЯ

Данное руководство предназначено для системных администраторов, осуществляющих развертывание, сопровождение и контроль функционирования программного средства "Средство виртуализации "РОСА Виртуализация 4" (версия 4.0) РСЮК.10103-01 (далее – РОСА Виртуализация).

В руководстве содержатся сведения о процессе, режимах, параметрах установки и первичной настройки РОСА Виртуализация.

Дополнительные сведения об администрировании РОСА Виртуализация приведены в документах:

– "РОСА Виртуализация 4. Руководство администратора. Часть 3. Эксплуатация" РСЮК.10103-01 32 03;
– "РОСА Виртуализация 4. Руководство администратора. Часть 4. Виртуальные машины" РСЮК.10103-01 32 04;
– "РОСА Виртуализация 4. Руководство администратора. Часть 5. Виртуальные рабочие места. Инфраструктура VDI" РСЮК.10103-01 32 05;
– "РОСА Виртуализация 4. Руководство администратора. Часть 6. Функции безопасности информации" РСЮК.10103-01 32 06;
– "РОСА Виртуализация 4. Руководство администратора. Часть 7. Руководство по системе резервного копирования" РСЮК.10103-01 32 07;
– "РОСА Виртуализация 4. Руководство пользователя. Портал виртуальных машин" РСЮК.10103-01 34 01.

Сведения о параметрах установки и первичной настройки РОСА Виртуализация с развертыванием СУСВ (Система управления средой виртуализации) на выделенном хосте приведены в документе "РОСА Виртуализация 4. Руководство администратора. Часть 2. Установка СУСВ на выделенном хосте" (индекс – РСЮК.10103-01 32 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" (индекс РСЮК.11001-02 90 01).

СОДЕРЖАНИЕ

1 Общие сведения....7
1.1 Назначение и функции....7
1.2 Область применения....7
1.3 Архитектура....7
1.4 Режимы функционирования....8
1.4.1 Промышленный режим....8
1.4.2 Тестовый режим....9
2 Условия выполнения установки....10
2.1 Требования к аппаратным средствам РОСА Виртуализация....10
2.1.1 Требования к серверу для установки гипервизора....10
2.1.2 Требования к серверу для установки сервера каталогов LDAP....11
2.2 Требования к межсетевому экрану и используемым портам....12
2.2.1 Требования к межсетевому экрану для DNS и NTP....12
2.2.2 Требования к межсетевому экрану СУСВ....12
2.2.3 Требования к межсетевому экрану хоста виртуализации....15
2.2.4 Требования к межсетевому экрану сервера базы данных....19
2.3 Требования к персоналу....20
3 Установка РОСА Виртуализация....21
3.1 Конфигурация установки РОСА Виртуализация....21
3.1.1 Стартовая конфигурация....21
3.1.2 Базовая конфигурация....21
3.2 Установка гипервизора на физический сервер....22
3.2.1 Подготовка к установке гипервизора с DVD....22
3.2.2 Подготовка к установке гипервизора с USB-накопителя....22
3.2.3 Запуск программы установки....29
3.2.4 Настройка параметров установки....32
3.2.5 Начало и ход процесса установки....61
3.2.6 Завершение установки....63
3.2.7 Вход в веб-интерфейс хоста гипервизора....66
3.3 Настройка системных параметров хоста гипервизора....68
3.3.1 Доступ к консоли с использованием веб-интерфейса....68
3.3.2 Доступ к консоли с использованием SSH....69

3.3.3 Разрешение имен DNS....70
3.3.4 Настройка аутентификации с применением криптографических ключей вместо пароля....71
3.4 Подготовка системы хранения данных....72
3.4.1 Подготовка хранилища NFS с использованием веб-интерфейса....73
3.4.2 Подготовка хранилища NFS с использованием командной строки....76
3.5 Установка СУСВ....78
3.5.1 Развертывание хранилища Gluster....79
3.5.2 Процесс установки виртуальной машины СУСВ....88
3.5.3 Очистка параметров установки СУСВ....102
3.5.4 Установка СУСВ в консольном режиме....103
3.5.5 Установка сертификата ЦС....103
3.5.6 Вход в веб-интерфейс СУСВ....114
3.6 Добавление хостов в кластер....118
3.6.1 Добавление хостов в кластер с использованием Портала администрирования СУСВ....119
3.7 Активация лицензии РОСА Виртуализация....121
3.7.1 Активация лицензии в веб-интерфейсе Портала администрирования 121
3.7.1.1 Установка ключа лицензии....122
3.7.1.2 Установка файла лицензии....125
3.7.1.3 Работа с лицензиями....128
3.7.2 Активация лицензии РОСА Виртуализация через интерфейс CLI....129
3.8 Установка сервера IPA....131
3.8.1 Создание ВМ для сервера IPA....131
3.8.2 Установка ОС на сервер IPA....136
3.8.3 Выполнение сценария установки ПО сервера IPA....140
3.8.4 Вход в веб-интерфейс сервера IPA....163
3.9 Подключение РОСА Виртуализация к службе каталогов LDAP сервера IPA 165
3.9.1 Создание системной учетной записи пользователя с использованием веб-интерфейса....166
3.9.1.1 Отображение активного системного пользователя....167
3.9.2 Создание профиля подключения к службе каталогов LDAP с помощью веб-интерфейса....174
3.9.2.1 Удаление LDAP-сервера....179

3.9.3 Создание профиля подключения к службе каталогов LDAP сервера IPA с помощью командной строки....180
3.9.4 Вход в Портал администрирования и Портал ВМ с использованием логина и пароля корпоративного LDAP-сервера....184
4 Развертывание внешнего Keycloak и интеграция с СУСВ....193
4.1 Развертывание внешнего Keycloak....193
4.1.1 Подготовка окружения....193
4.1.2 Установка и настройка дополнительного ПО....194
4.1.3 Настройка Keycloak....197
4.2 Интеграция СУСВ с внешним Keycloak....213
4.2.1 Отображение состояния интеграции....215
4.2.2 Настройка и активация интеграции....218
4.2.3 Откат интеграции....228
4.3 Управление доступом в СУСВ интегрированном с внешним Keycloak....230
4.3.1 Управление пользователями в Keycloak....231
4.3.2 Импорт пользователей и групп в СУСВ....234
Перечень сокращений....237

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение и функции

РОСА Виртуализация – средство виртуализации с интегрированной системой управления, предназначенная для развертывания и эксплуатации виртуального центра обработки данных (ВЦОД) корпоративного уровня.

РОСА Виртуализация 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

РОСА Виртуализация может эксплуатироваться в центрах обработки данных государственных органов и частных организаций различного масштаба.

Версия РОСА Виртуализация, 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 РОСА Виртуализация 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 РОСА Виртуализация. Наиболее распространенными режимами функционирования являются промышленный и тестовый режимы.

1.4.1 Промышленный режим

Промышленный режим функционирования РОСА Виртуализация 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 РОСА Виртуализация 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 РОСА Виртуализация используется для развертывания средства виртуализации в лабораториях и учебных классах с целью создания стенда для изучения функций и демонстрации возможностей РОСА Виртуализация.

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

– 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 РОСА Виртуализация 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 РОСА Виртуализация

В базовой конфигурации установки аппаратное обеспечение РОСА Виртуализация 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 РОСА Виртуализация);

– 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 и NTP

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

По умолчанию РОСА Виртуализация разрешает исходящий трафик на DNS и NTP на любом адресе назначения. Если требуется отключить исходящий трафик, то нужно определить исключения для запросов, которые отправляются на DNS и NTP серверы.

Рекомендации и требования:

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

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

– Вместо файла /etc/hosts рекомендуется использовать DNS 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, открыть 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 можно 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, т. к. 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 отключить исходящий трафик, нужно сделать исключения для СУСВ, чтобы он отправлял запросы на DNS- и NTP-серверы. Другие узлы также могут требовать DNS и NTP. В этом случае следует ознакомиться с требованиями для этих узлов и настроить 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 (таблица 2).

Чтобы отключить автоматическую настройку межсетевого экрана при добавлении нового хоста, нужно снять 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

			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 требуется 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 Linux	Хосты виртуализации Хосты ROSA Linux	Миграция виртуальной машины с использованием libvirt	Да
H9	49152 - 4921	TCP	Хосты виртуализац	Хосты виртуализации	Миграция и ограждение виртуальных	Да. В зависимости от агента

	5		ии Хосты ROSA Linux	Хосты ROSA Linux	машин с использованием VDSM. Эти порты должны быть открыты для облегчения как автоматизированной, так и ручной миграции виртуальных машин	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
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 отключить исходящий трафик, нужно сделать 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 следует ознакомиться с требованиями для этих узлов и настроить межсетевой экран соответствующим образом.

2.2.4 Требования к межсетевому экрану сервера базы данных

POCA Виртуализация поддерживает использование удаленного сервера базы данных для базы данных СУСВ (engine) и базы данных Data Warehouse (ovirt-engine-history). Если планируется использование удаленного сервера базы данных, он должен разрешать соединения из СУСВ и службы Data Warehouse (которая может быть отдельной от СУСВ).

Аналогично, если планируется получение доступа 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.

Описанная в таблице 3 конфигурация межсетевого экрана предполагает конфигурацию по умолчанию.

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 РОСА Виртуализация, 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 РОСА ВИРТУАЛИЗАЦИЯ

Установка РОСА Виртуализация осуществляется администратором в соответствии с заранее выбранной конфигурацией установки – стартовой или базовой.

3.1 Конфигурация установки РОСА Виртуализация

3.1.1 Стартовая конфигурация

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

Для установки РОСА Виртуализация в стартовой конфигурации выполняют следующие действия:

а) установка гипервизора и настройка системных параметров на хосте;

б) подготовка системы хранения данных;

в) установка СУСВ;

г) активация лицензии РОСА Виртуализация.

3.1.2 Базовая конфигурация

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

Для установки РОСА Виртуализация в базовой конфигурации выполняют следующие действия:

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

б) подготовка системы хранения данных;

в) установка СУСВ;

г) добавление хостов в кластер;

д) активация лицензии РОСА Виртуализация;

е) установка сервера IPA в качестве сервера каталогов LDAP для идентификации и аутентификации доменных пользователей и настройка подключения РОСА Виртуализация к службе каталогов LDAP сервера IPA.

3.2 Установка гипервизора на физический сервер

Установка гипервизора РОСА Виртуализация 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 дистрибутива с DVD;
– установка дистрибутива с ISO-образа, предварительно записанного на USB-накопитель.

3.2.1 Подготовка к установке гипервизора с DVD

По умолчанию дистрибутив РОСА Виртуализация поставляется на DVD.

При наличии у сервера DVD-привода установка осуществляется с DVD, на который записан дистрибутив РОСА Виртуализация.

Необходимо установить DVD с записанным на него дистрибутивом в DVD-накопитель и перейти 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 РОСА Виртуализация на USB-накопитель, используя DVD 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, нужно выполнить следующие шаги в терминале Linux:

а) убедиться, что файлы myfile.iso и myile.sha256 загружены и находятся в одной директории;

б) выполнить команду `sha256sum` вместе с опцией "-c", чтобы проверить контрольную сумму:

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

Для дистрибутива РОСА Виртуализация, выпущенного 16.01.2026 (файл RV-4.0-20260116.0-rv-x86_64-dvd1.iso), команда выглядит следующим образом:

```
$ sha256sum -c RV-4.0-20260116.0-rv-x86_64-dvd1.sha256
```

Если контрольная сумма совпадает, появится сообщение, подобное этому:

```
  myfile.iso: OK
```

или

```
  myfile.iso: ЦЕЛ
```

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

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

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

Пример проверки контрольной суммы в консоли:

```
$ sha256sum -c RV-4.0-20260116.0-rv-x86_64-dvd1.sha256
```

```
RV-4.0-20260116.0-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 можно использовать команду:

```
$ sudo yum install gostsum
```

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

а) убедиться, что файлы myfile.iso и myfile.gost12 загружены и находятся в одной директории;

б) выполнить команду `gost12sum`, чтобы подсчитать контрольную сумму:

```
$ gost12sum myfile.iso
```

Для дистрибутива РОСА Виртуализация, выпущенного 16.01.2026 (файл RV-4.0-20260116.0-rv-x86_64-dvd1.iso), команда выглядит следующим образом:

```
$ gost12sum RV-4.0-20260116.0-rv-x86_64-dvd1.iso
```

в) вывести контрольную сумму, сохраненную в файл myfile.gost12, используя команду `cat`:

```
$ cat myfile.gost12
```

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

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

Пример подсчёта контрольной суммы в консоли:

```
$ gost12sum RV-4.0-20260116.0-rv-x86_64-dvd1.iso
```

```
    20d7c130fe377d593c2502e29ff4091f0040e4ce33eecb31220da30a7bdb
cac0 RV-4.0-20260116.0-rv-x86_64-dvd1.iso
```

Пример вывода ранее сохранённой контрольной суммы в консоль:

```
    $ cat RV-4.0-20260116.0-rv-x86_64-dvd1.gost12
    20d7c130fe377d593c2502e29ff4091f0040e4ce33eecb31220da30a7bdb
cac0 RV-4.0-20260116.0-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 РОСА Виртуализация. Возможно установить на любой компьютер или сервер РОСА Виртуализация в минимальной конфигурации или использовать любой хост РОСА Виртуализация.

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

```
    # hostnamectl | grep "Operating System"
      Operating System: РОСА Виртуализация 4.0
```

В данном случае на хосте установлена РОСА Виртуализация, и она может быть использована для проверки контрольной суммы.

Следует убедиться, что установлен пакет OpenSSL:

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

Если пакет OpenSSL установлен, то можно переходить к следующим шагам.

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

а) убедиться, что файлы myfile.iso и myfile.gost12 загружены и находятся в одной директории;

б) выполнить команду `openssl`, чтобы подсчитать контрольную сумму:

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

Для дистрибутива РОСА Виртуализация, выпущенного 16.01.2026 (файл RV-4.0-20260116.0-rv-x86_64-dvd1.iso), команда выглядит следующим образом:

```
$ openssl dgst -streebog256 RV-4.0-20260116.0-rv-x86_64-dvd1.iso
```

в) вывести контрольную сумму, сохраненную в файл, используя команду `cat`:

```
$ cat myfile.gost12
```

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

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

Пример подсчёта контрольной суммы в консоли:

```
$ openssl dgst -streebog256 RV-4.0-20260116.0-rv-x86_64-dvd1.iso
md_gost12_256(RV-4.0-20260116.0-rv-x86_64-dvd1.iso)= 20d7c130fe377d593c2502e29ff4091f0040e4ce33eecb31220da30a7bdbcac0
```

Контрольная сумма выводится после знака "=".

Пример вывода ранее сохранённой контрольной суммы в консоль:

```
$ cat RV-4.0-20260116.0-rv-x86_64-dvd1.gost12
20d7c130fe377d593c2502e29ff4091f0040e4ce33eecb31220da30a7bdbcac0 RV-4.0-20260116.0-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 РОСА Виртуализация на USB-накопитель в ОС Linux

Для записи образа нужно вставить диск с дистрибутивом РОСА Виртуализация в DVD-привод, подключить USB-накопитель и скопировать 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 на USB-накопитель в других операционных системах следует обратиться к Руководству пользователя конкретной операционной системы.

Важно – Для выполнения указанных ниже команд необходимы права суперпользователя (администратора) системы. Если права на выполнение операций с диском на уровне администратора отсутствуют, следует обратиться к администратору системы.

На компьютере с установленной ОС семейства Linux для копирования диска нужно выполнить 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 выполняют 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 нужно загрузить сервер с носителя с дистрибутивом РОСА Виртуализация.

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

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

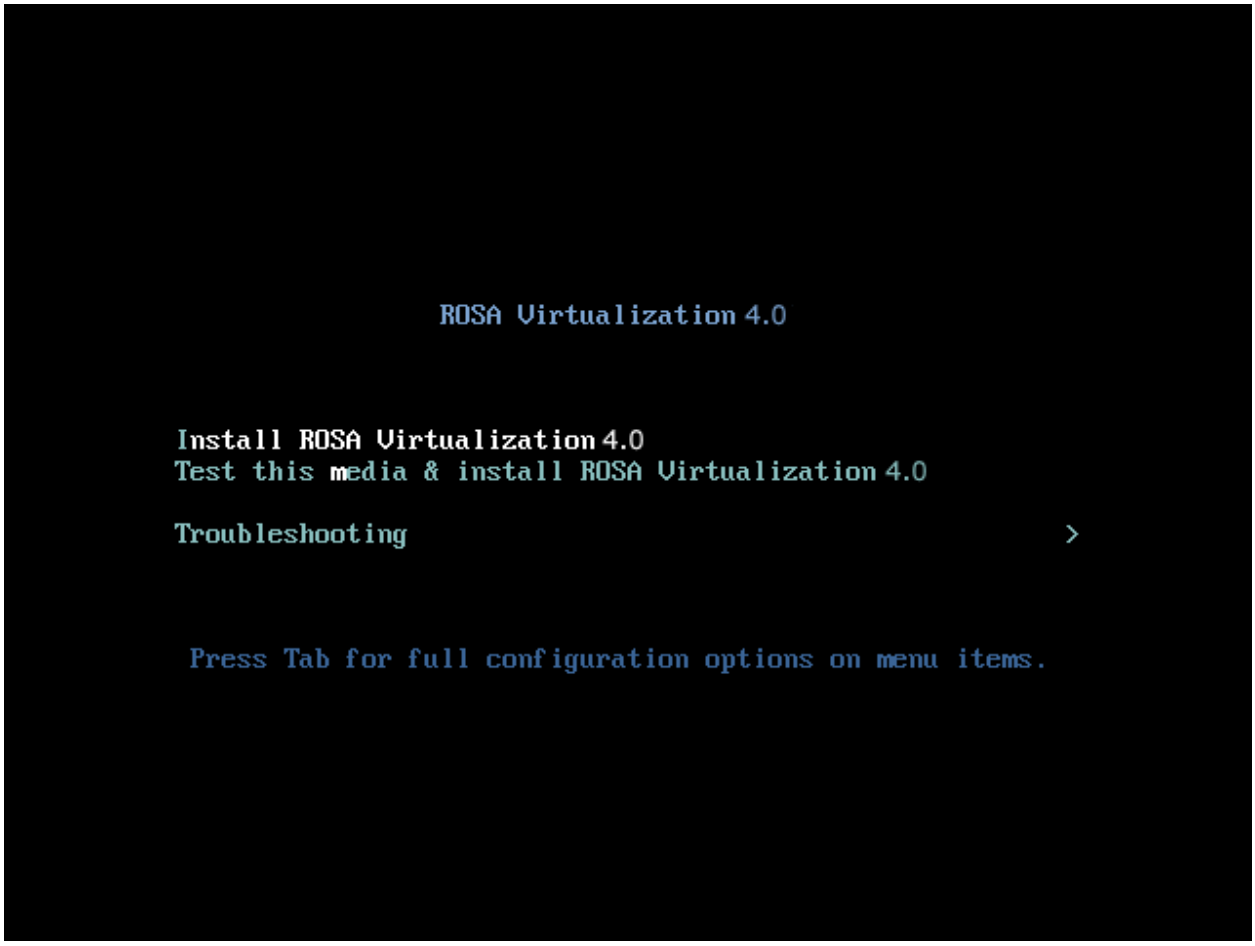

Рисунок 1 – Меню установки РОСА Виртуализация

Для запуска графического интерфейса программы установки гипервизора нужно нажать клавишу `Enter` или дождаться 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 требуется нажать клавишу `Tab`, затем ввести через пробел слово "`text`" в конец строки с параметрами загрузки и нажать 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.

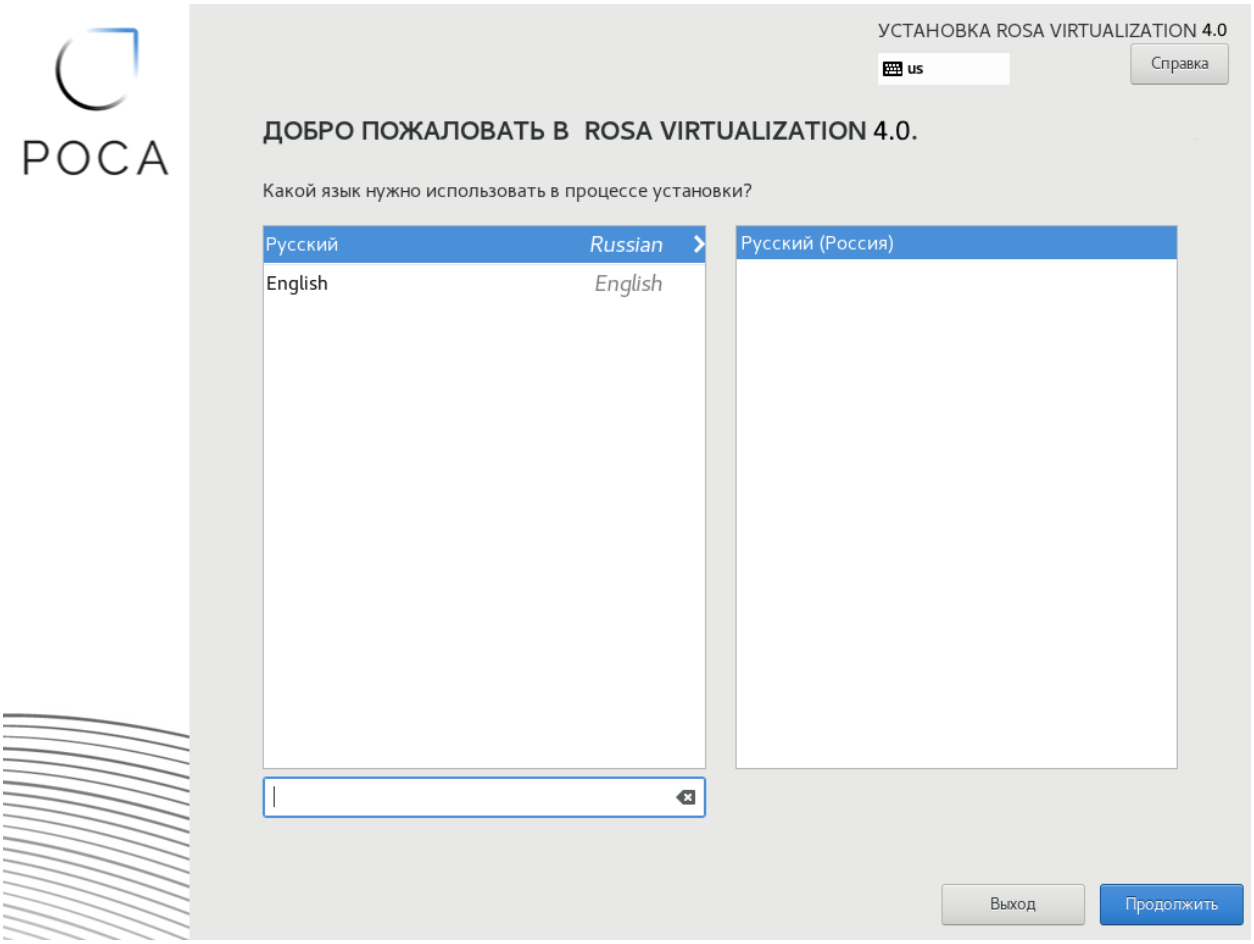

Рисунок 2 – Окно приветствия программы установки

Используя полосу прокрутки и строку поиска нужно выбрать 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 необходимо нажать кнопку Продолжить.

3.2.4 Настройка параметров установки

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 в меню "Обзор установки" (рисунок 3).

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".

Для перехода к интерфейсу настройки соответствующих параметров следует нажать на наименование секции.

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

– Дата и время (см. пункт 3.2.4.1.1);
– Место установки (см. пункт 3.2.4.4.1);
– Имя сети и узла (см. пункт 3.2.4.5);
– Пароль root (см. пункт 3.2.4.2).

Примечание – Настройка "Дата и время" с использованием серверов NTP требует подключения к внешним сетевым источникам точного времени. "Имя сети и узла" рекомендуется настроить до начала настройки "Дата и время", если планируется использовать внешние сетевые источники точного времени.

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

Для отмены установки необходимо нажать кнопку Выход и подтвердить прекращение процесса установки.

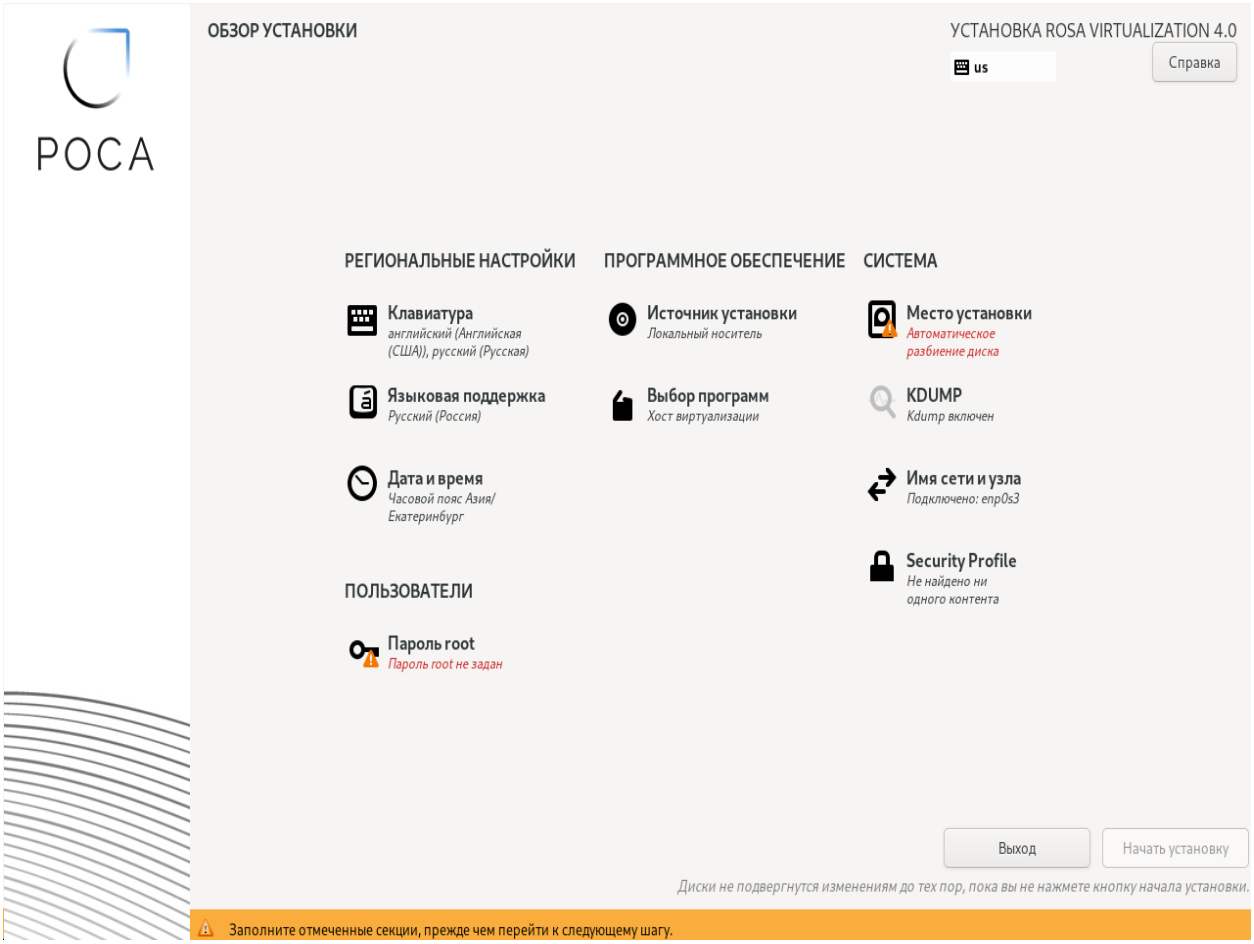

Рисунок 3 – Обзор установки

В меню "Обзор установки" параметры установки распределены по следующим разделам – "Региональные настройки", "Пользователи", "Программное обеспечение", "Система".

3.2.4.1 Региональные настройки

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

– Клавиатура – 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 – предназначена для добавления дополнительных языков в пользовательский интерфейс гипервизора. Значение параметра по умолчанию – "Русский (Россия)";

– Дата и время – предназначена 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.

3.2.4.1.1 Дата, время и часовой пояс

В секции "Дата и время" можно выполнить настройку даты, времени и часового пояса, а также подключение гипервизора к внешним сетевым источникам точного времени по протоколу NTP (рисунок 4).

Важно – Для настройки с использованием серверов NTP требуется настроенное сетевое подключение (настройка осуществляется в секции "Имя сети и узла"), обеспечивающее сетевую доступность серверов NTP.

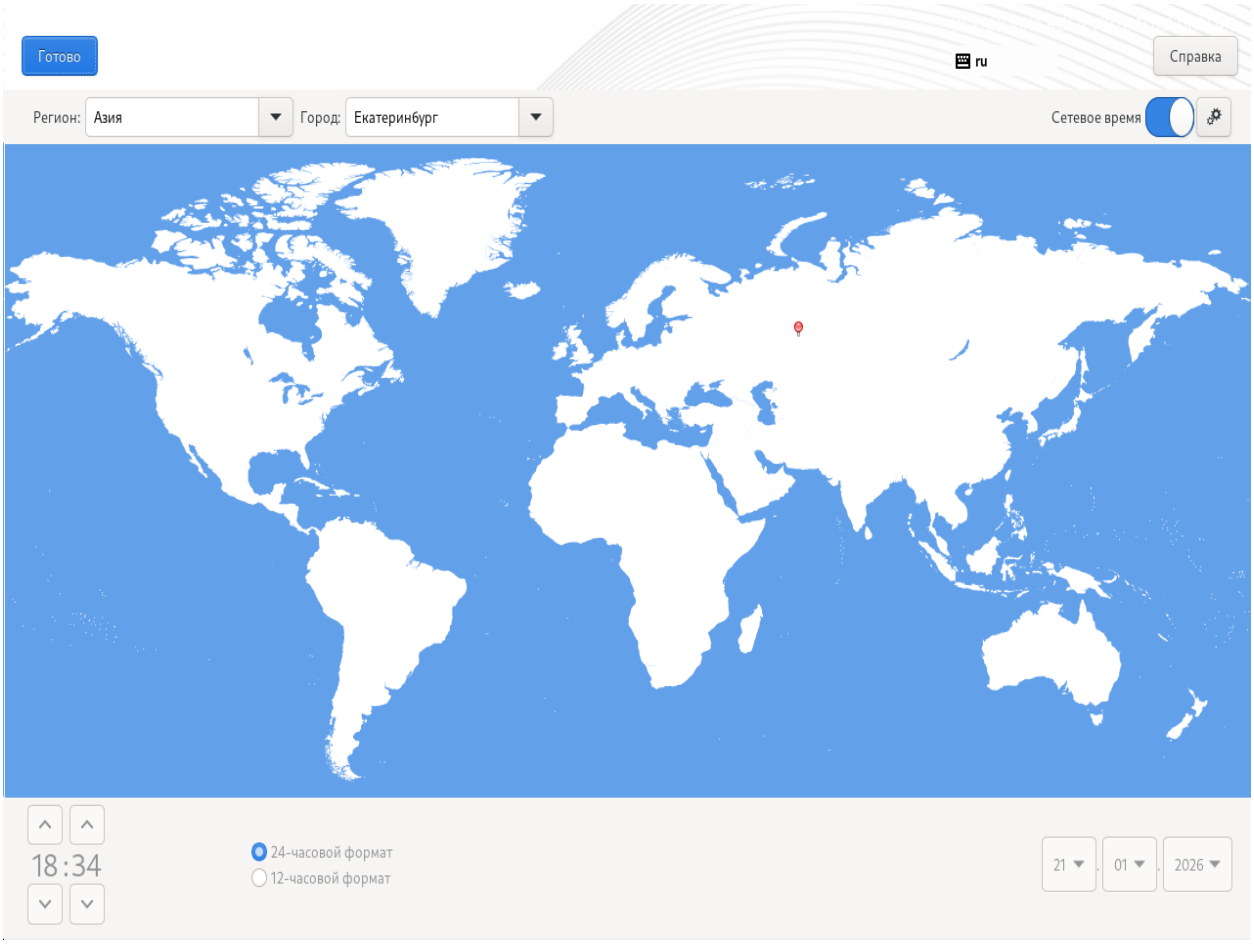

Рисунок 4 – Настройка даты, времени и часового пояса

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

Важно – Часовой пояс следует настроить, даже если планируется использовать протокол NTP для синхронизации часов.

Если системные часы показывают неверное время, можно откорректировать его с помощью кнопок ∧ (больше) и ∨ (меньше). Для выбора формата отображения времени нужно отметить нужный режим – 24-часовой формат или 12-часовой формат.

При необходимости можно скорректировать дату, выбрав 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.

3.2.4.1.2 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, нужно установить во включенное положение переключатель "Сетевое время".

Для настройки синхронизации времени с определенным сервером NTP необходимо нажать кнопку конфигурации . На экране появится диалоговое окно "Добавить и отметить используемые серверы NTP" (рисунок 5).

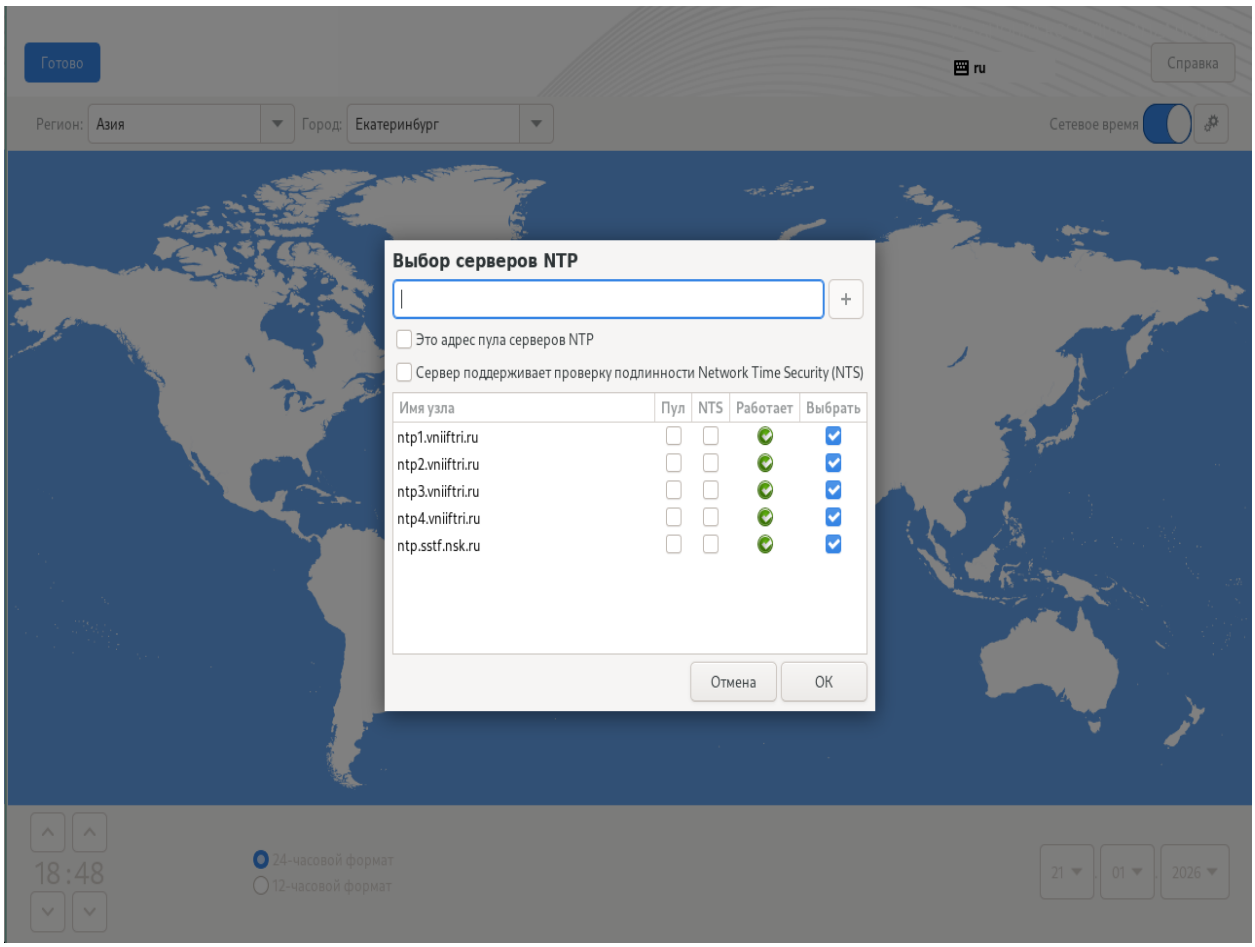

Рисунок 5 – Выбор серверов NTP

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

Для выбора сервера NTP из списка нужно установить флажок "Выбрать".

Для добавления дополнительного сервера NTP в список следует ввести имя узла (адрес) и нажать кнопку +. Для завершения настройки нажать кнопку ОК (рисунок 5).

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

После настройки параметров даты и времени необходимо нажать кнопку Готово для возвращения в меню "Обзор установки".

3.2.4.2 Пользователи

Раздел "Пользователи" содержит секцию "Пароль root", которая предназначена для настройки учетной записи root (администратора гипервизора).

В секции можно настроить следующие параметры:

– Пароль к учетной записи администратора (root);
– Заблокировать учетную запись root;
– Разрешить вход пользователем root через SSH.

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

– При выборе и использовании пароля рекомендуется следовать следующим правилам:

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

– В окне секции "Пароль root" необходимо ввести и подтвердить пароль для учетной записи суперпользователя (рисунок 6).

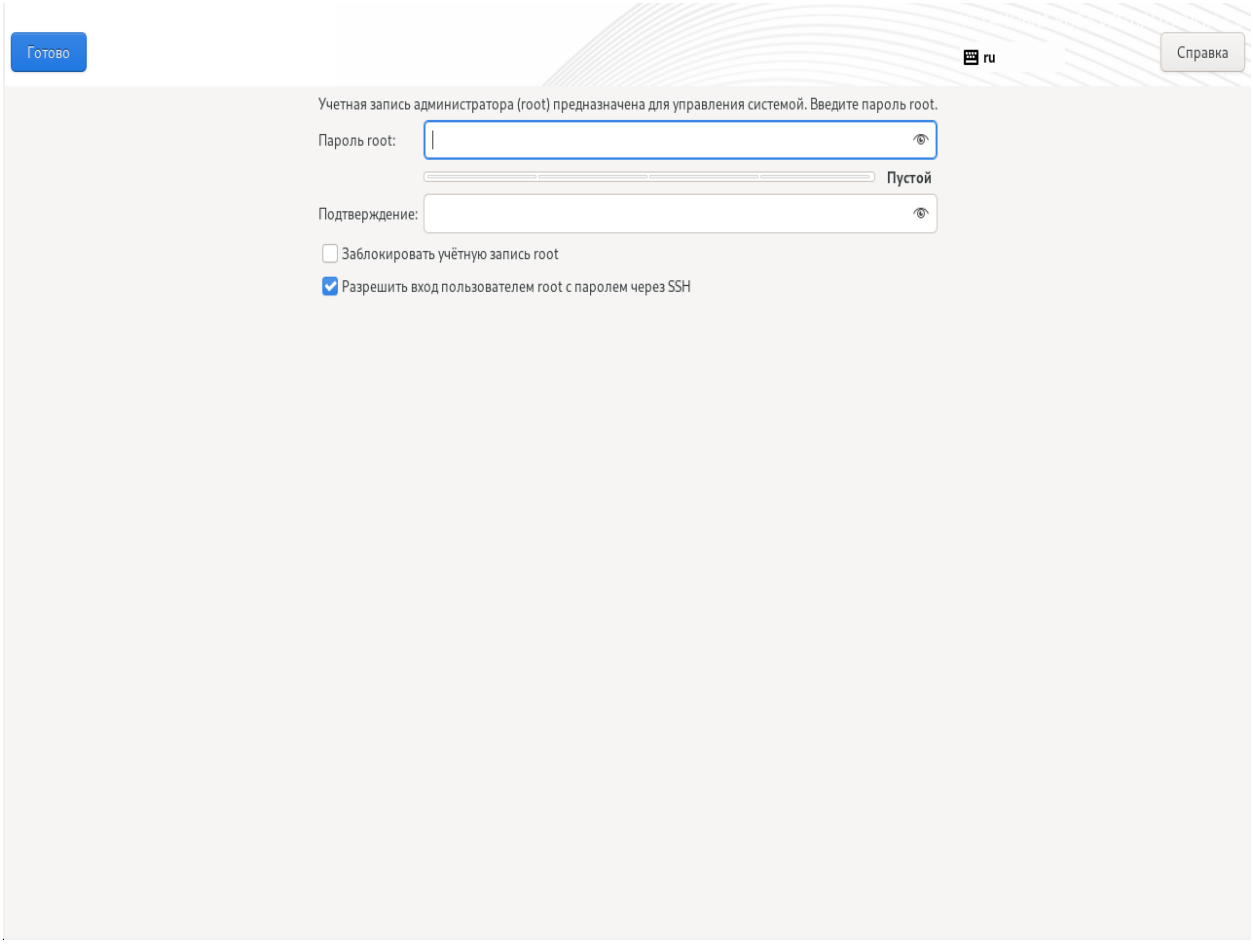

Рисунок 6 – Ввод и подтверждение пароля учетной записи root

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

После завершения настройки нужно нажать кнопку Готово для возвращения в меню "Обзор установки".

3.2.4.3 Программное обеспечение

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

– Источник установки – 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 – предназначена 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 программ

Тип и набор устанавливаемого программного обеспечения можно выбрать в секции "Выбор программ" (рисунок 7).

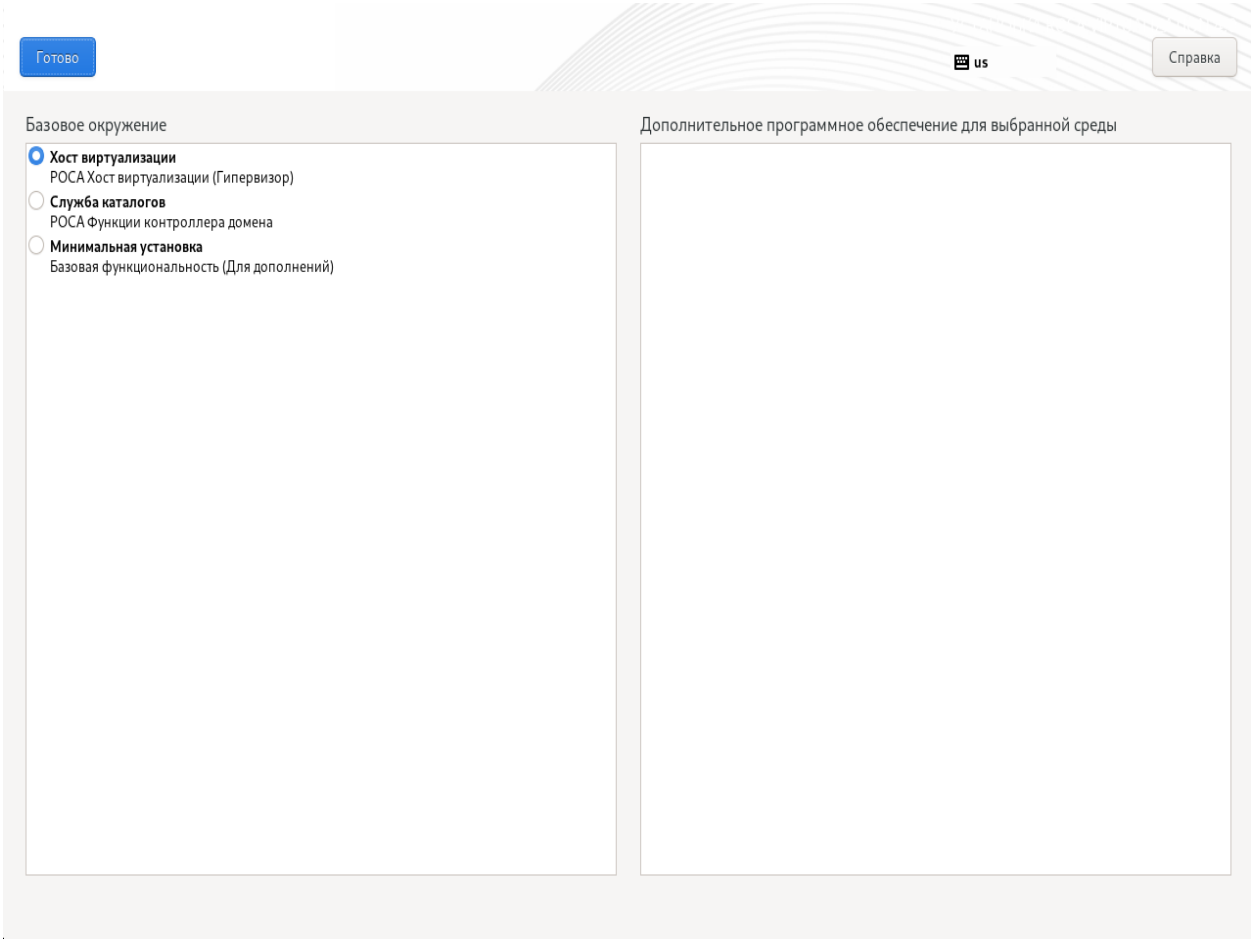

Рисунок 7 – Выбор типа устанавливаемого ПО (выбран Хост виртуализации)

Для выбора доступны следующие типы базового окружения:

– Хост виртуализации – для установки хоста виртуализации (функции гипервизора);

– Служба каталогов – для установки службы каталогов/контроллера домена;

– Минимальная установка – для установки минимальной конфигурации сервера.

После выбора необходимо нажать на кнопку Готово для возврата на экранную форму "Обзор установки".

3.2.4.4 Система

Раздел "Система" содержит следующие секции с параметрами установки:

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

– KDUMP – предназначена для управления (включение/выключение) и настройки резервирования памяти для kdump (механизм сбора статистики о сбоях ядра). Значение параметров по умолчанию:"kdump" — включен, "Резервирование памяти kdump" - Автоматически;

– Имя сети и узла – предназначена для настройки параметров сетевых адаптеров и указания имени хоста гипервизора;

– Security Profile – предназначена для настройки параметров получения контента профиля безопасности.

3.2.4.4.1 Место установки

Интерфейс секции "Место установки" предназначен для выбора диска для установки гипервизора и настройки конфигурации разделов диска в автоматическом или ручном режиме (рисунок 8).

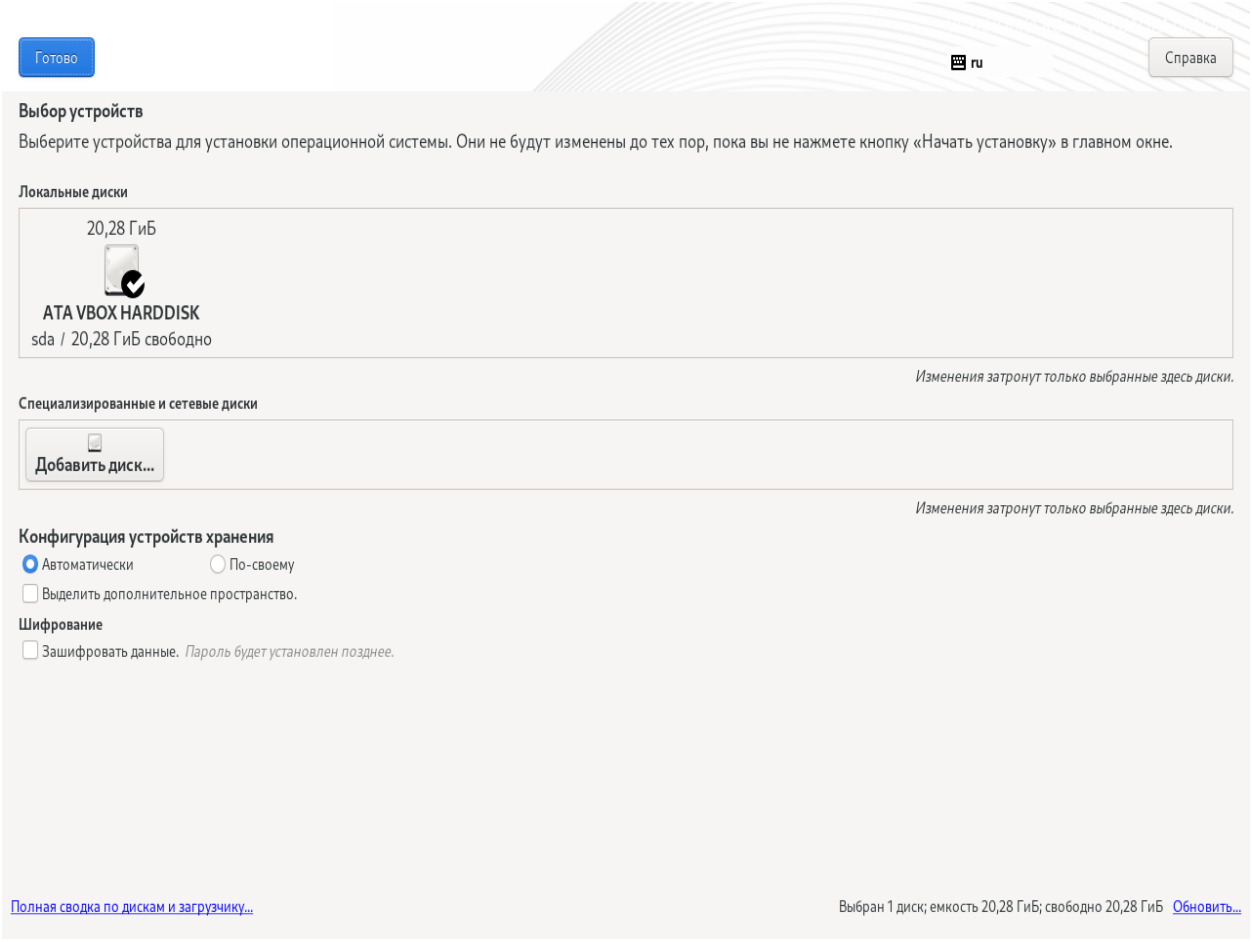

Рисунок 8 – Выбор диска и способа конфигурации разделов

По умолчанию интерфейс отображает только локальные диски, доступные для установки гипервизора. Для каждого диска показаны размер, метка, доступное пространство. Для выбора диска нужно нажать на блок с информацией о диске. Выбранный для установки диск будет отмечен флажком. При необходимости и наличии можно выбрать 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) нажимают кнопку Добавить диск.

Для новой установки гипервизора с удалением всех существующих данных с выбранного диска нужно установить переключатель "Конфигурация устройств хранения" в положение "Автоматически". Если на выбранном диске недостаточно свободного места для автоматического разбиения или был установлен флажок "Выделить дополнительное пространство", следует освободить пространство на диске вручную (см. пункт 3.2.4.4.1.1).

Для настройки пользовательской конфигурации и создания разделов диска требуется вручную установить переключатель "Конфигурация устройств хранения" в положение "По-своему" (см. пункт 3.2.4.4.1.2).

Примечание – При необходимости в шифровании разделов диска (кроме /boot) устанавливают флажок "Зашифровать данные" (см. пункт 3.2.4.4.2).

При наличии двух и более дисков, выбранных для установки гипервизора, следует перейти по ссылке "Полная сводка по дискам и загрузчику" в интерфейс выбора диска, на котором будет установлен загрузчик (см. пункт 3.2.4.4.3).

Для продолжения настройки конфигурации диска или возвращения в меню "Обзор установки" нужно нажать кнопку Готово.

3.2.4.4.1.1. Освобождение дополнительного пространства на диске

Интерфейс освобождения дискового пространства содержит список разделов диска (файловых систем) и элементы управления, позволяющие удалять или уменьшать разделы (рисунок 9).

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.

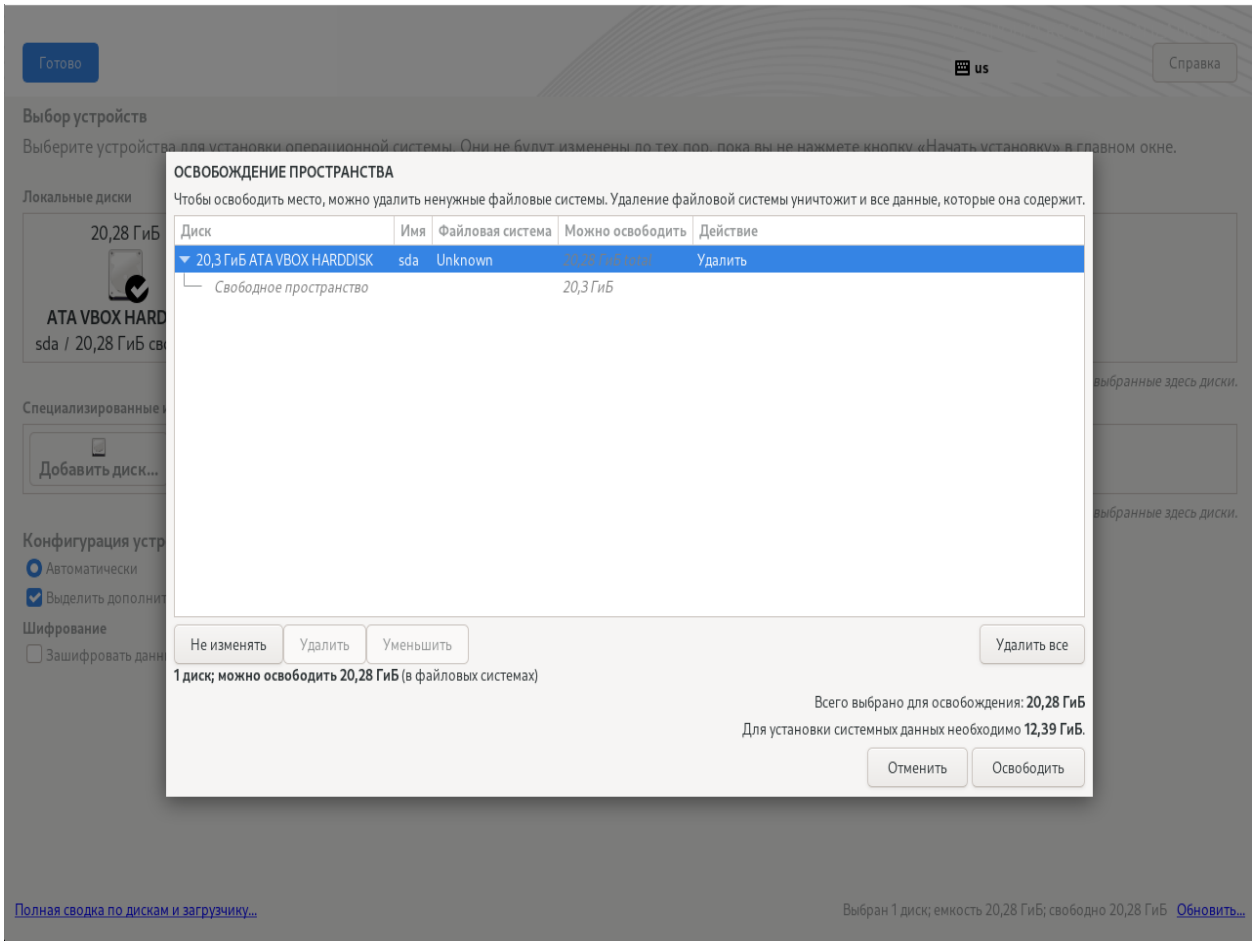

Рисунок 9 – Интерфейс формы для освобождения дискового пространства

В столбце "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.

Перед применением требуемых методов освобождения пространства необходимо выбрать файловую систему (раздел) или весь диск,. Когда будет достигнут достаточный объем свободного дискового пространства для продолжения установки (объем зависит от выбранного базового и дополнительного ПО), нужно нажать кнопку Освободить пространство, которая станет доступной для использования (Рисунок 10).

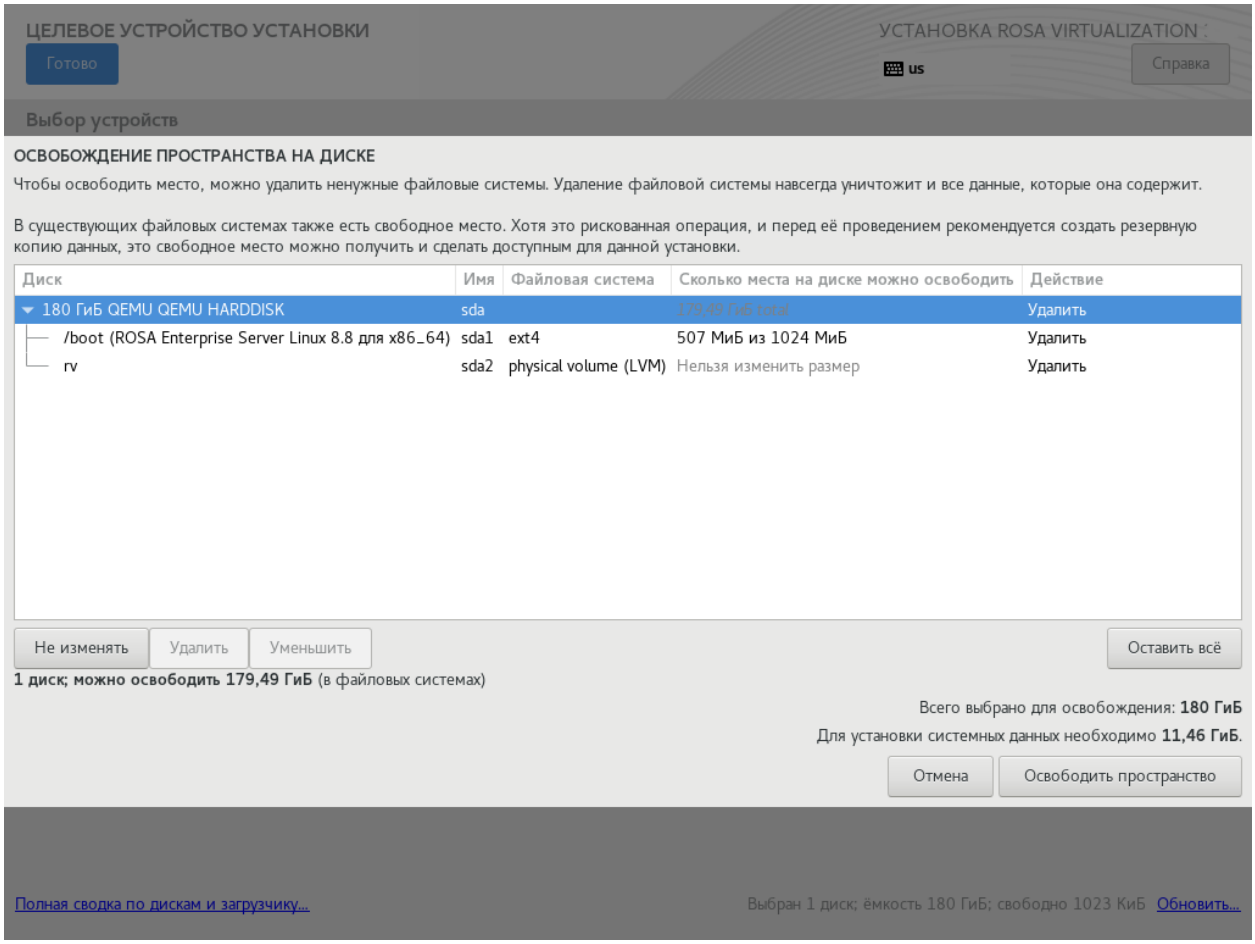

Рисунок 10 – Выбрано для освобождения 180ГБ дискового пространства

3.2.4.4.1.2. 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" был установлен в положение "По-своему", на экране появится интерфейс создания разделов диска.

3.2.4.4.1.3 Создание схемы разделов "Динамический LVM"

Для создания схемы разделов "Динамический LVM" нужно выбрать в списке пункт "Динамический LVM" (рисунок 11).

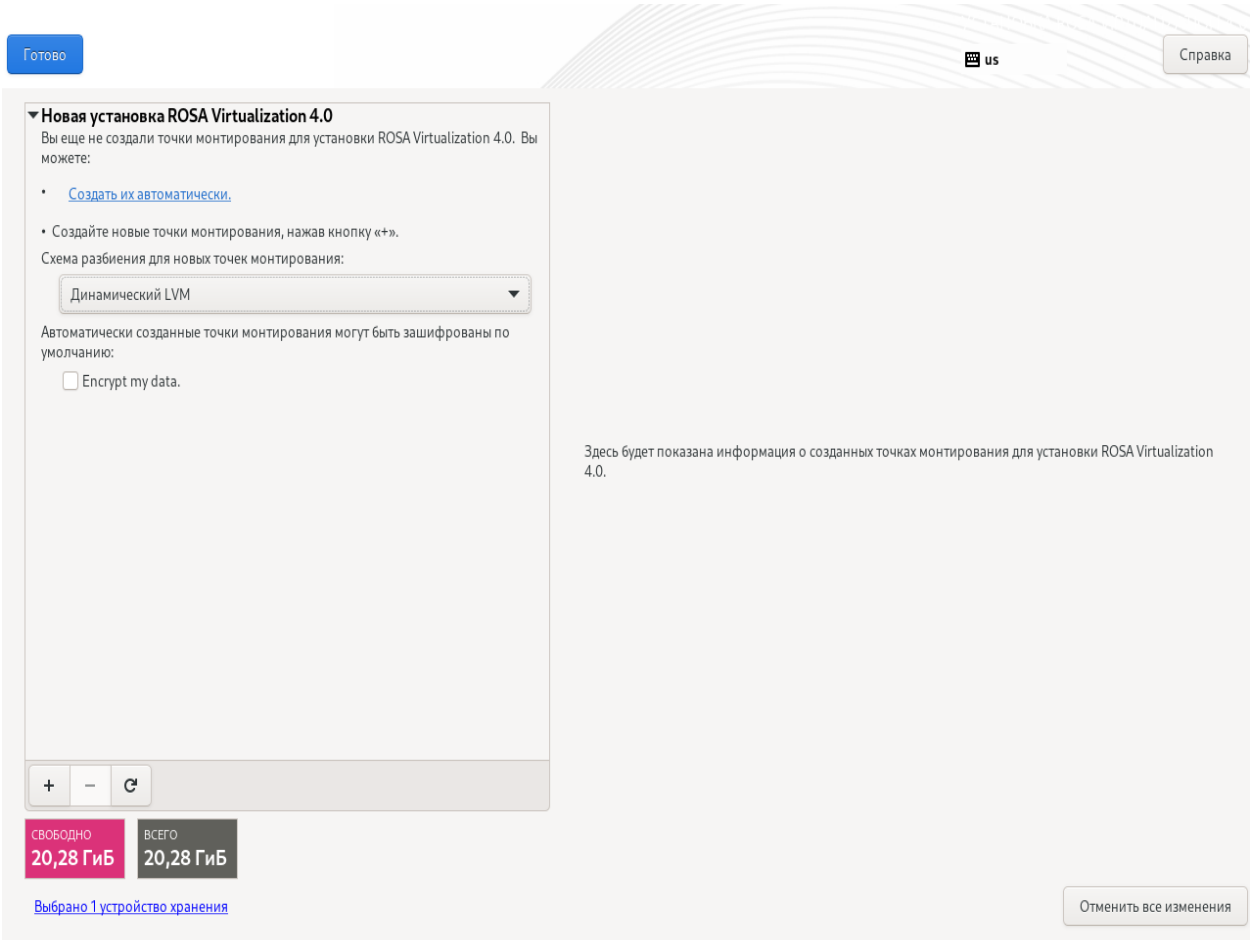

Рисунок 11 – Создание схемы разделов "Динамический LVM"

3.2.4.4.1.4 Создание стандартных разделов

Для создания схемы со стандартными разделами нужно выбрать в списке пункт "Стандартный раздел" (рисунок 12).

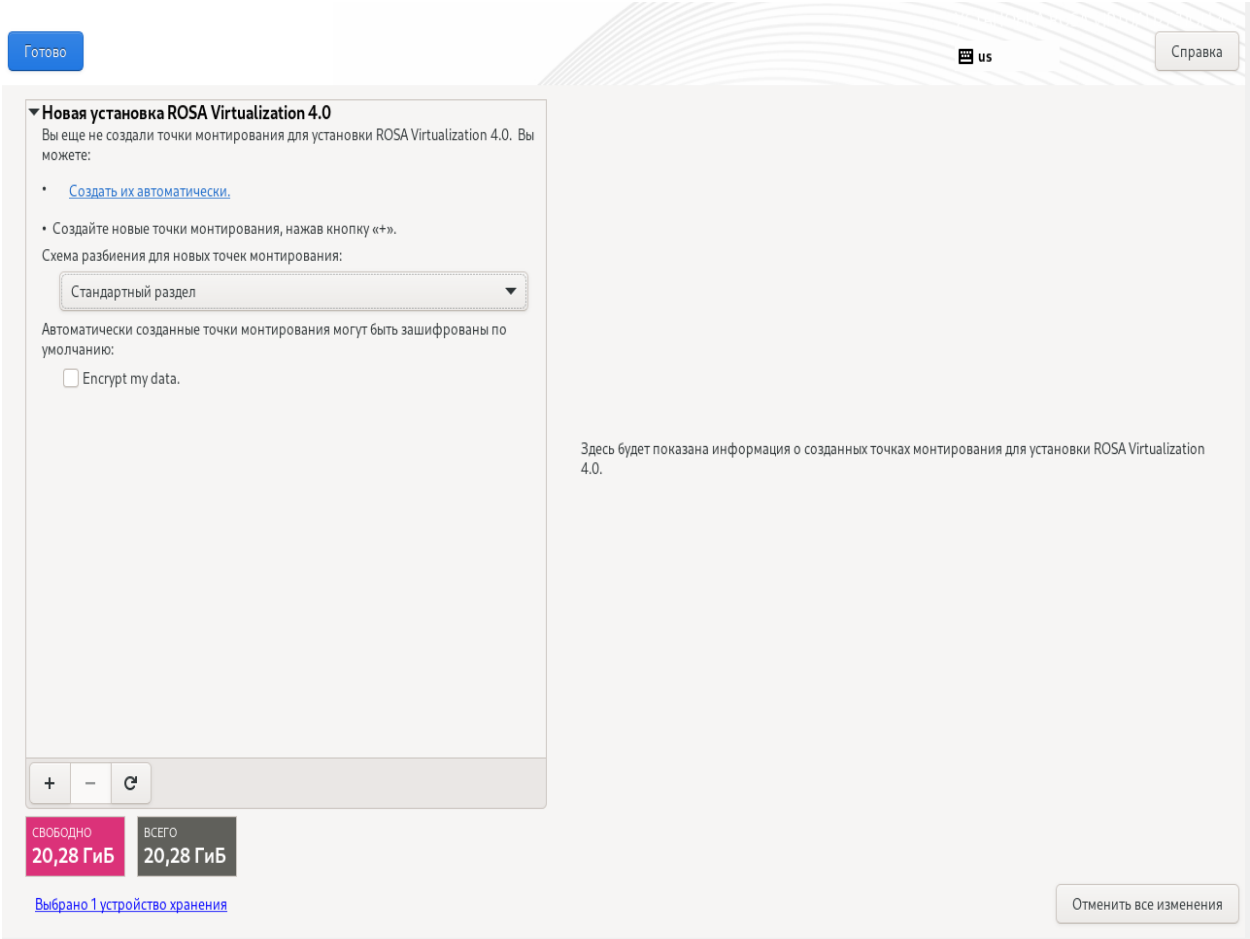

Рисунок 12 – Создание схемы со стандартными разделами

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

3.2.4.4.1.5 Автоматическое создание разделов и точки монтирования

Для того чтобы программа установки автоматически создала разделы и точки монтирования, нужно выбрать схему разбиения разделов – "Стандартный раздел", "Динамический LVM" (схема по умолчанию), "LVM" – из выпадающего списка и нажать 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.

3.2.4.4.1.6 Создание точки монтирования вручную

Для создания точки монтирования вручную нужно:

а) нажать кнопку +. На экране появится модальное окно "Создание точки монтирования" (рисунок 13);

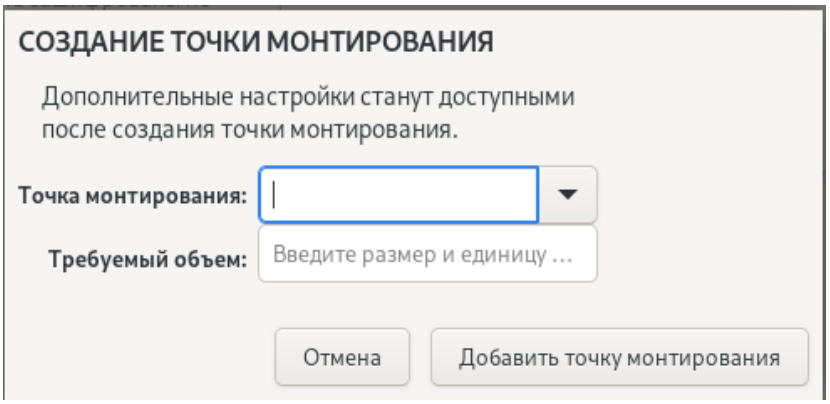

Рисунок 13 – Создание точки монтирования

б) выбрать раздел для подключения точки монтирования из выпадающего списка в поле "Точка монтирования" (рисунок 13) или ввести путь к необходимому разделу вручную. Например, / – для корневого раздела, /boot – для загрузочного раздела;

в) указать 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;

г) нажать кнопку Добавить точку монтирования (рисунок 13).

После создания точки монтирования станут доступными (в правой области интерфейса) настройки параметров раздела (рисунок 14).

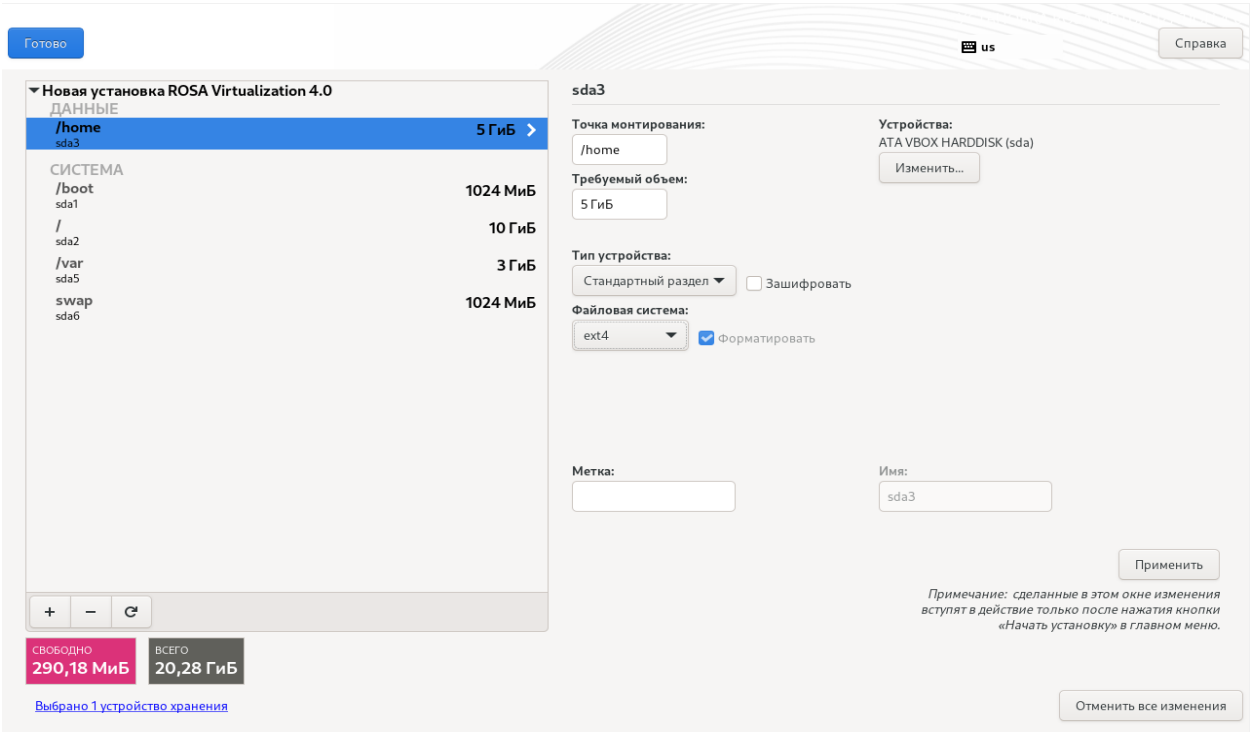

Рисунок 14 – Настройки параметров раздела

Для выбранного раздела доступны следующие параметры настройки:

– Точка монтирования – точка подключения раздела. Например, для корневого раздела вводят "/", для загрузочного раздела – "/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", "Динамический LVM" (см. пункт 3.2.4.4.1.8). 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 3.2.4.4.1.11). 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 изменить значения параметров.

Для сохранения изменений необходимо нажать кнопку Применить. При этом изменения вступят в силу только после начала установки.

Для завершения настройки нужно нажать кнопку Готово.

На экране появится модальное окно "Обзор изменений" (рисунок 15), где будут перечислены выбранные операции по настройке разделов и файловых систем, включающие создание, изменение размера и удаление.

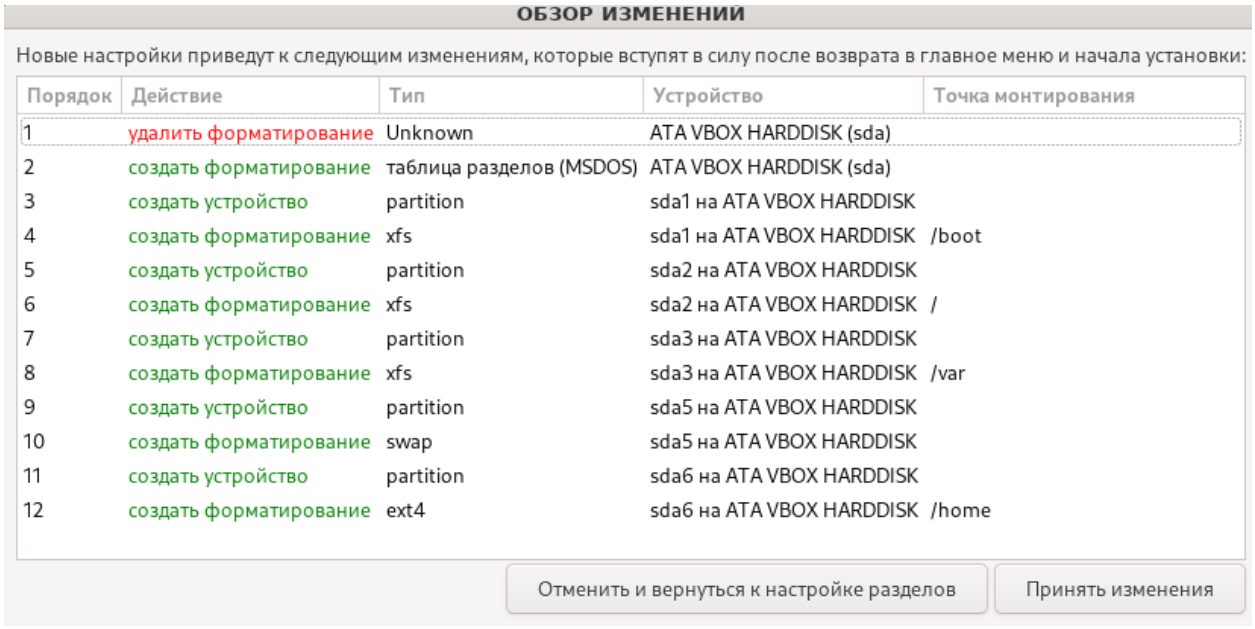

Рисунок 15 – Озор изменений

Для сохранения необходимо нажать кнопку Принять изменения.

Для отмены изменений можно нажать кнопку Отменить и вернуться к настройке разделов.

Для того чтобы настроить разделы вручную на другом диске, нужно выбрать необходимый диск в окне интерфейса секции "Место установки" и установить переключатель "Конфигурация устройств хранения" в положение "По-своему".

3.2.4.4.1.7 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.

3.2.4.4.1.8 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;

– Динамический LVM – раздел перераспределяет свободное пространство между устройствами в зависимости от требований приложений. По мере необходимости пул пространства может наращиваться динамически (см. пункт 3.2.4.4.1.9);

– 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 3.2.4.4.1.10).

3.2.4.4.1.9 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 выполнением следующих действий:

а) из выпадающего списка "Тип устройства" выбрать значение "Динамический LVM". В результате появится список "Группа Томов" с именем созданной группы томов LVM;

б) для настройки созданной группы томов LVM нажать кнопку Изменить. На экране появится модальное окно "Настройка группы томов" (рисунок 16);

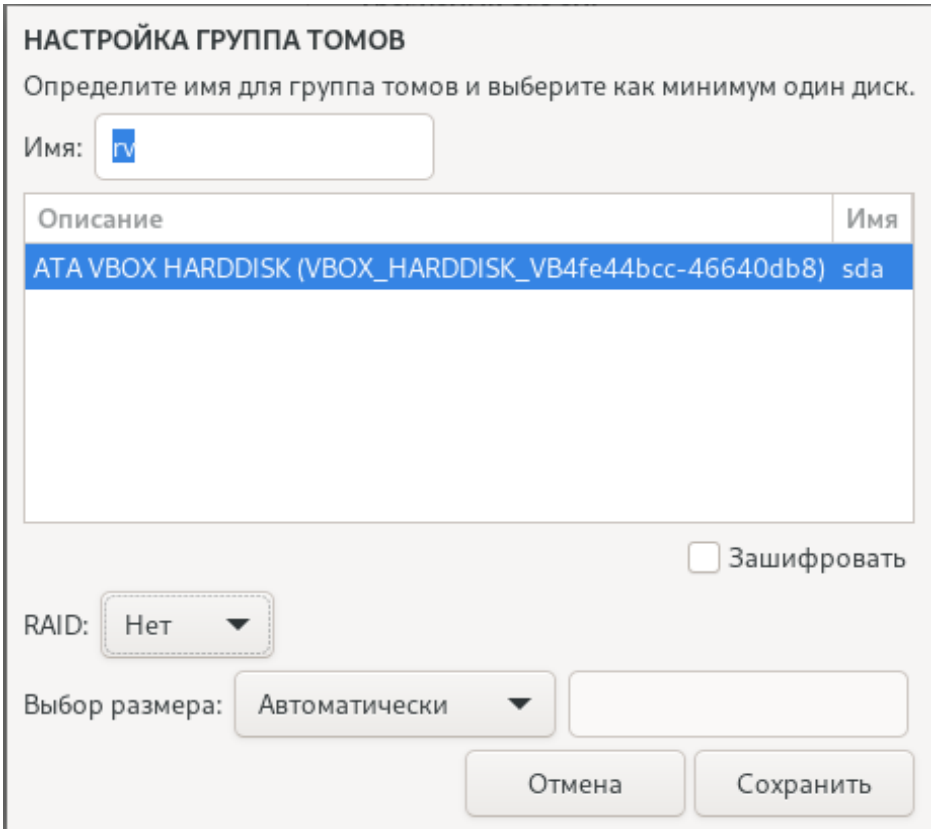

Рисунок 16 – Настройка группы томов LVM

в) ввести имя для группы томов LVM и выбрать диск/диски для размещения раздела;

г) при необходимости создать программный RAID-массив для группы томов LVM (см. пункт 3.2.4.4.1.10); выбрав из выпадающего списка "RAID" 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 установливают флажок "Зашифровать".

д) определить размер группы томов LVM, выбрав из выпадающего списка "Выбор размера" 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;

– Фиксирован – точный размер группы томов устанавливается вручную – ввести в поле необходимое значение размера группы томов;

е) нажать кнопку Сохранить.

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

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

3.2.4.4.1.10 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" нужно выбрать 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 необходимо нажать кнопку Применить.

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

3.2.4.4.1.11 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.

3.2.4.4.2 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 "Место установки" был установлен флажок "Зашифровать данные", на экране появится интерфейс создания пароля доступа к зашифрованным данным (рисунок 17).

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

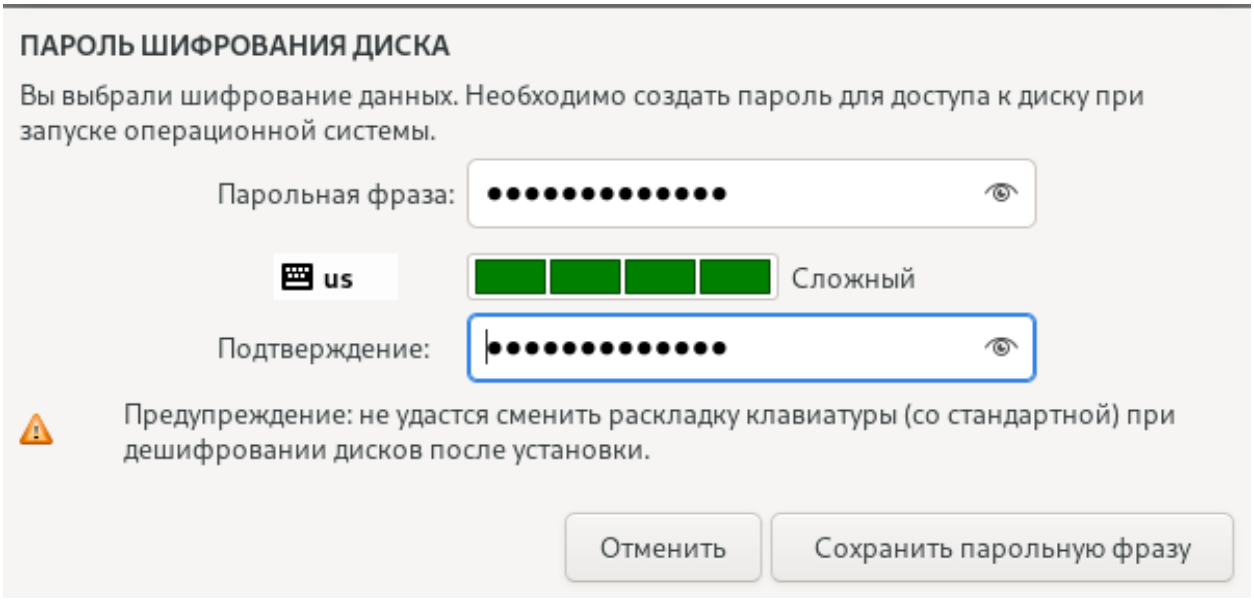

Рисунок 17 – Создание пароля доступа при использовании шифрования диска

В поле "Парольная фраза" нужно ввести парольную фразу, при этом обратив внимание на раскладку клавиатуры (рисунок 17). Для изменения раскладки клавиатуры нужно нажать на значок . Если введенный пароль является слабым, на экране появится информационное сообщение с предупреждением.

В поле "Подтверждение" следует ввести пароль доступа еще раз, после чего нажать кнопку `Сохранить парольную фразу`.

3.2.4.4.3 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 18). Переход по ссылке "Полная сводка по дискам и загрузчику" откроет интерфейс выбора диска, на котором будет установлен загрузчик.

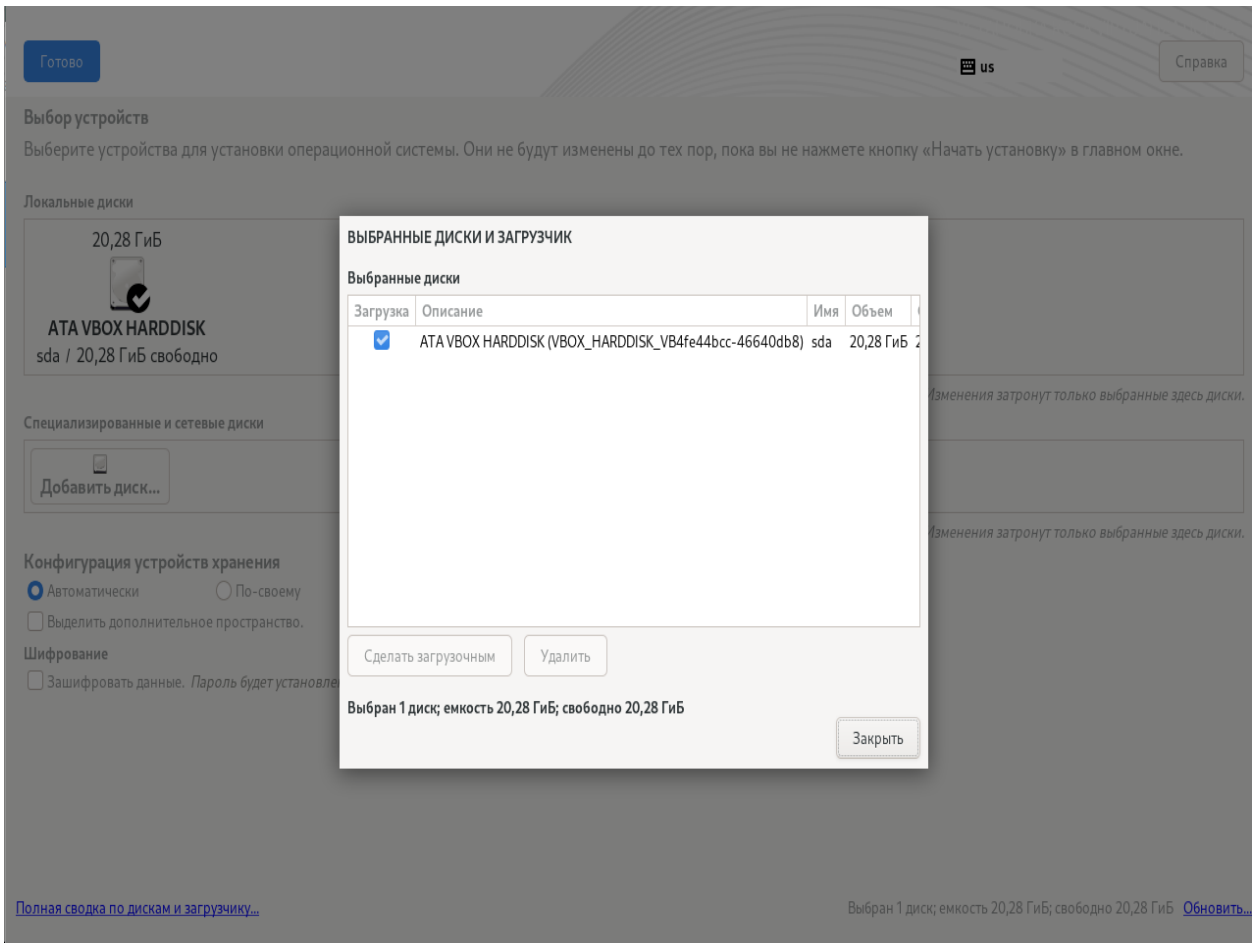

Рисунок 18 – Выбор диска для установки загрузчика

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

Для возвращения к интерфейсу секции "Место установки" требуется нажать кнопку `Закрыть` (рисунок 18).

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.

3.2.4.5 Имя сети и узла

Интерфейс секции "Имя сети и узла" предназначен для указания имени хоста и настройки параметров сетевых адаптеров гипервизора (рисунок 19).

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

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

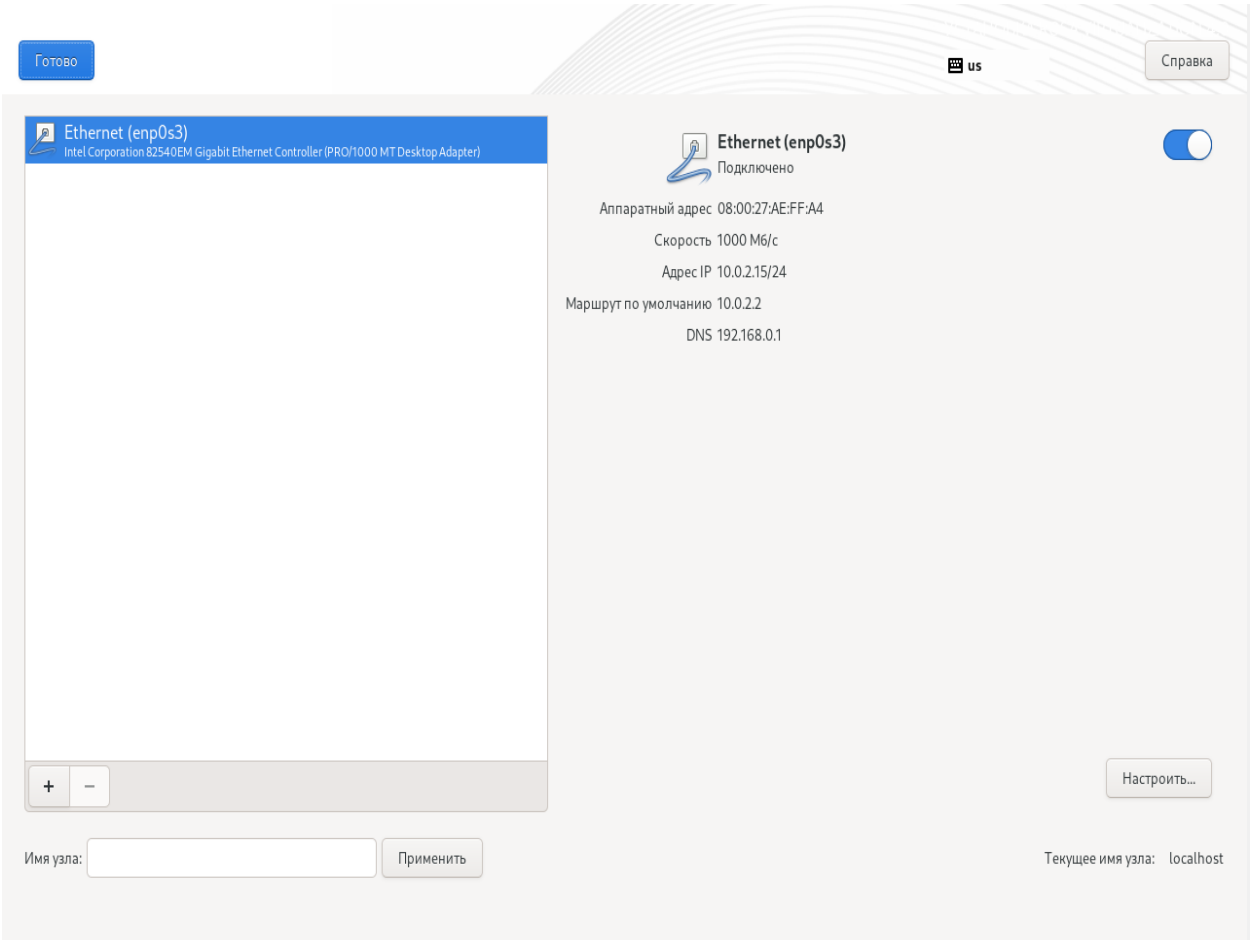

Рисунок 19 – Сетевые адаптеры и имя узла

3.2.4.5.1 Имя узла

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

В поле "Имя узла" нужно ввести полное доменное имя хоста гипервизора (например, "rvhost1.rosa.lan") и нажать 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.

3.2.4.5.2 Сетевые подключения

Программа установки гипервизора автоматически найдет доступные сетевые интерфейсы и отобразит их списком в левой части окна секции "Имя сети и узла".

Для подключения/отключения сетевого интерфейса нужно выбрать необходимый адаптер в списке и установить переключатель, расположенный в правом верхнем углу, в соответствующее положение.

Для настройки параметров нужно выбрать необходимый сетевой интерфейс в списке и нажать кнопку Настроить. На экране появится окно с параметрами интерфейса (перечень доступных параметров зависит от типа сетевого соединения) (рисунок 20).

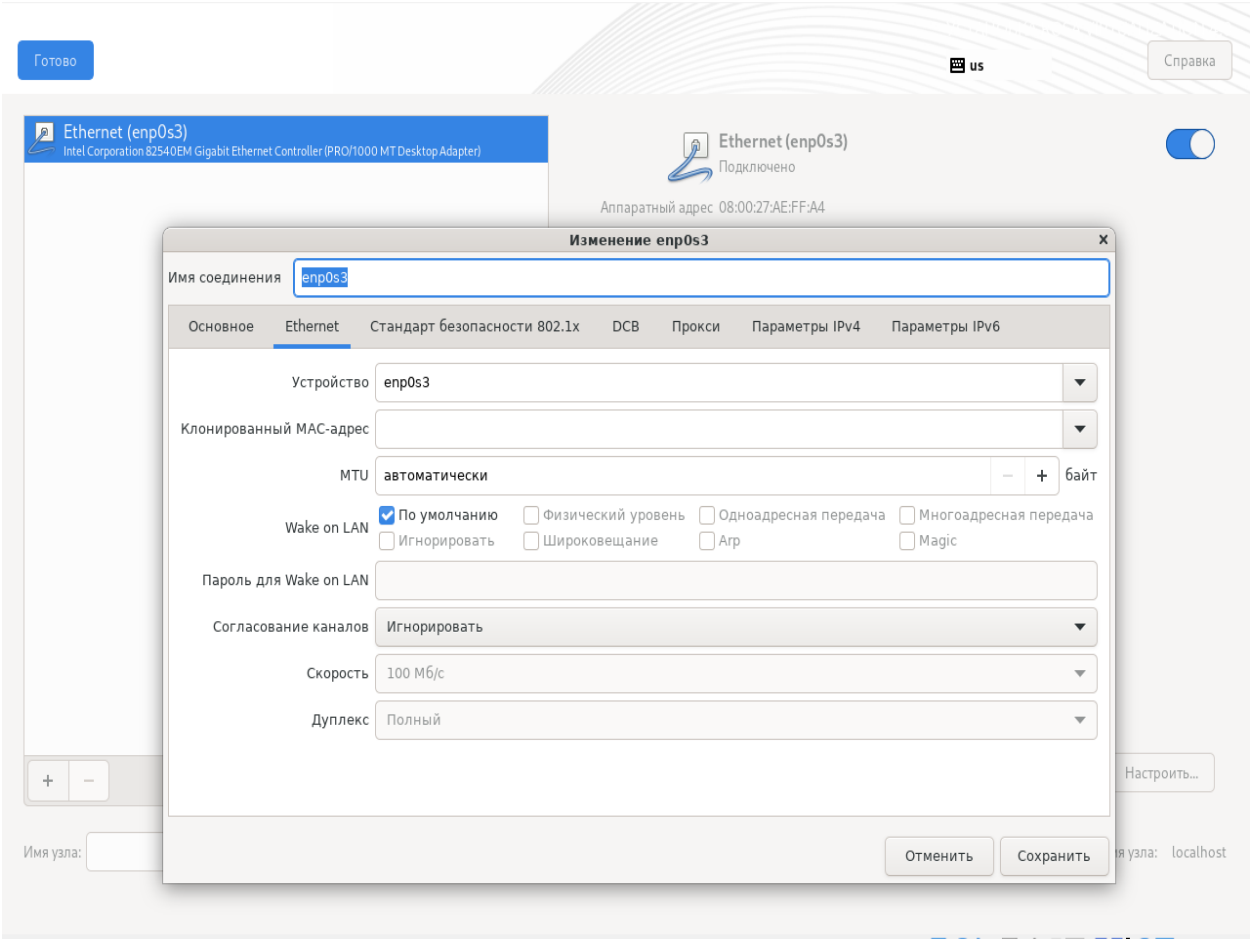

Рисунок 20 – Параметры сетевого соединения: IPv4, подключение вручную, "Требовать адресацию IPv4 для этого соединения"

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

3.2.4.5.2.1 Настройка параметров сетевого подключения с автоматическим конфигурированием по протоколу DHCP

По умолчанию сетевые параметры IPv4 и IPv6 настраиваются автоматически по протоколу DHCP (рисунок 21).

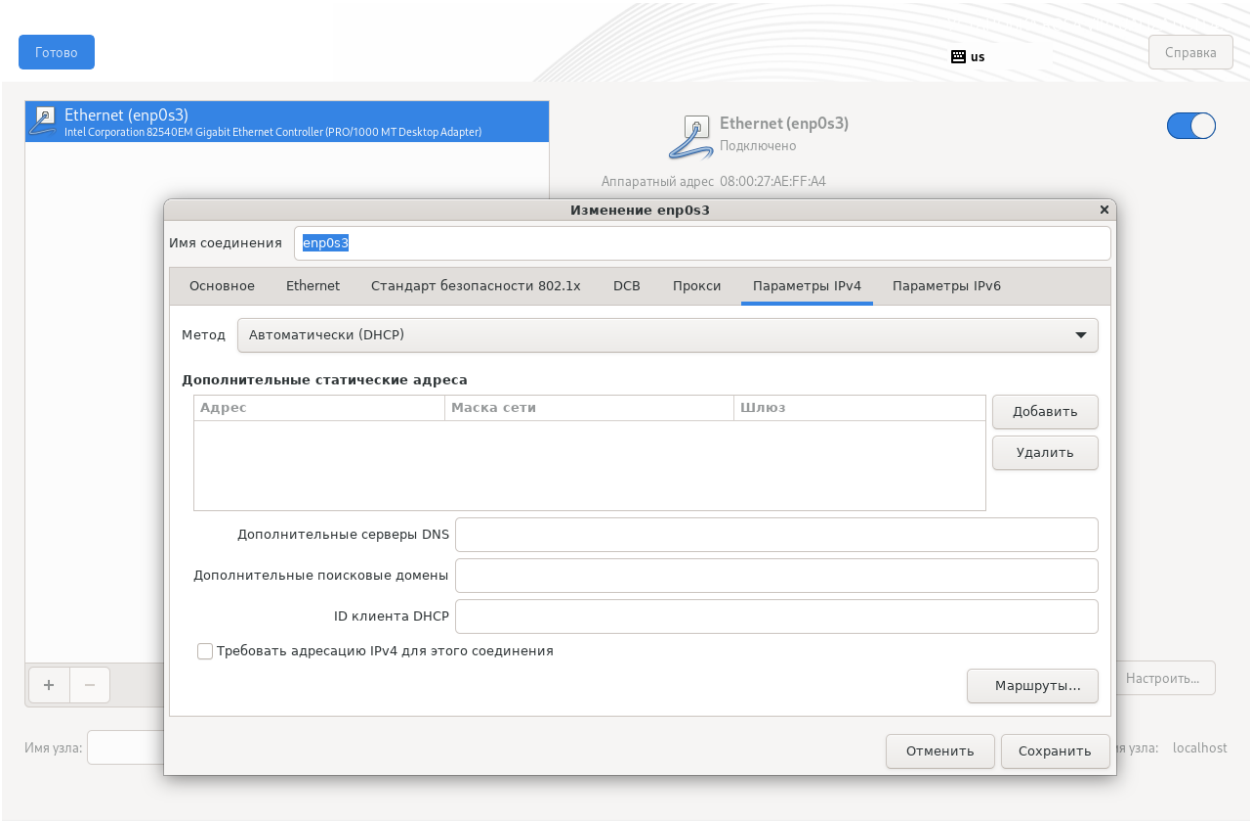

Рисунок 21 – Настройка IPv4 с автоматическим конфигурированием по протоколу DHCP

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.

3.2.4.5.2.2 Настройка параметров сетевого подключения с использованием статического IP-адреса

Для настройки сетевого соединения с использованием статического IP-адреса нужно:

а) перейти на вкладку "Параметры IPv4" и выбрать из выпадающего списка "Метод" значение "Вручную" (рисунок 22);

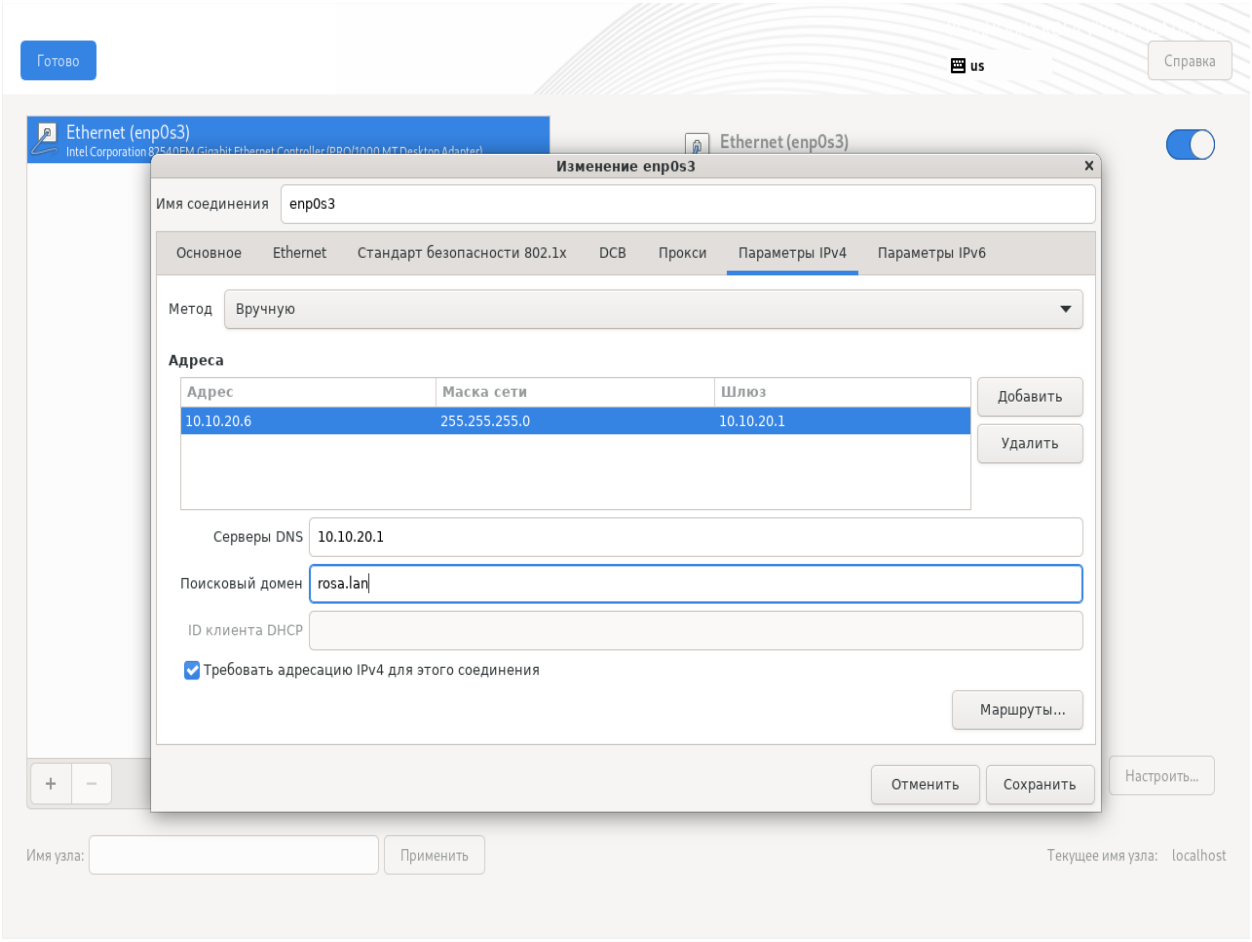

Рисунок 22 – Настройка параметров IPv4: вручную (статический IP-адрес), IP-адрес, маска подсети, шлюз, DNS-сервер, шлюз и поисковый домен

б) нажать кнопку Добавить и ввести в соответствующие поля необходимые значения статического IP-адреса интерфейса, маски сети и шлюза;

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

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

г) в поле "Поисковый домен" указать наименование домена (например, "rosa.lan");

д) установить флажок "Требовать адресацию IPv4 для этого соединения";

е) для применения сделанных изменений нажать кнопку Сохранить (рисунок 22);

ж) для добавления и настройки нового сетевого интерфейса нажать кнопку + в левой нижней части окна секции "Имя сети и узла";

з) для удаления выбранного сетевого интерфейса из списка программы установки нажать кнопку –;

и) после настройки сетевых параметров нажать кнопку Готово для возвращения в меню "Обзор установки" (рисунок 22).

Все работы с сетевыми интерфейсами VLAN необходимо выполнять в графическом интерфейсе СУСВ после развертывания Системы и настройки кластера. Если управляющая сеть ovirtmgmt должна быть тегированной изначально, то после установки гипервизора, но до развертывания СУСВ, следует внести изменения в интерфейс физического сетевого устройства непосредственно на хосте, прописав в нем параметры VLAN, как указано в п. 3.2.6.

3.2.5 Начало и ход процесса установки

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

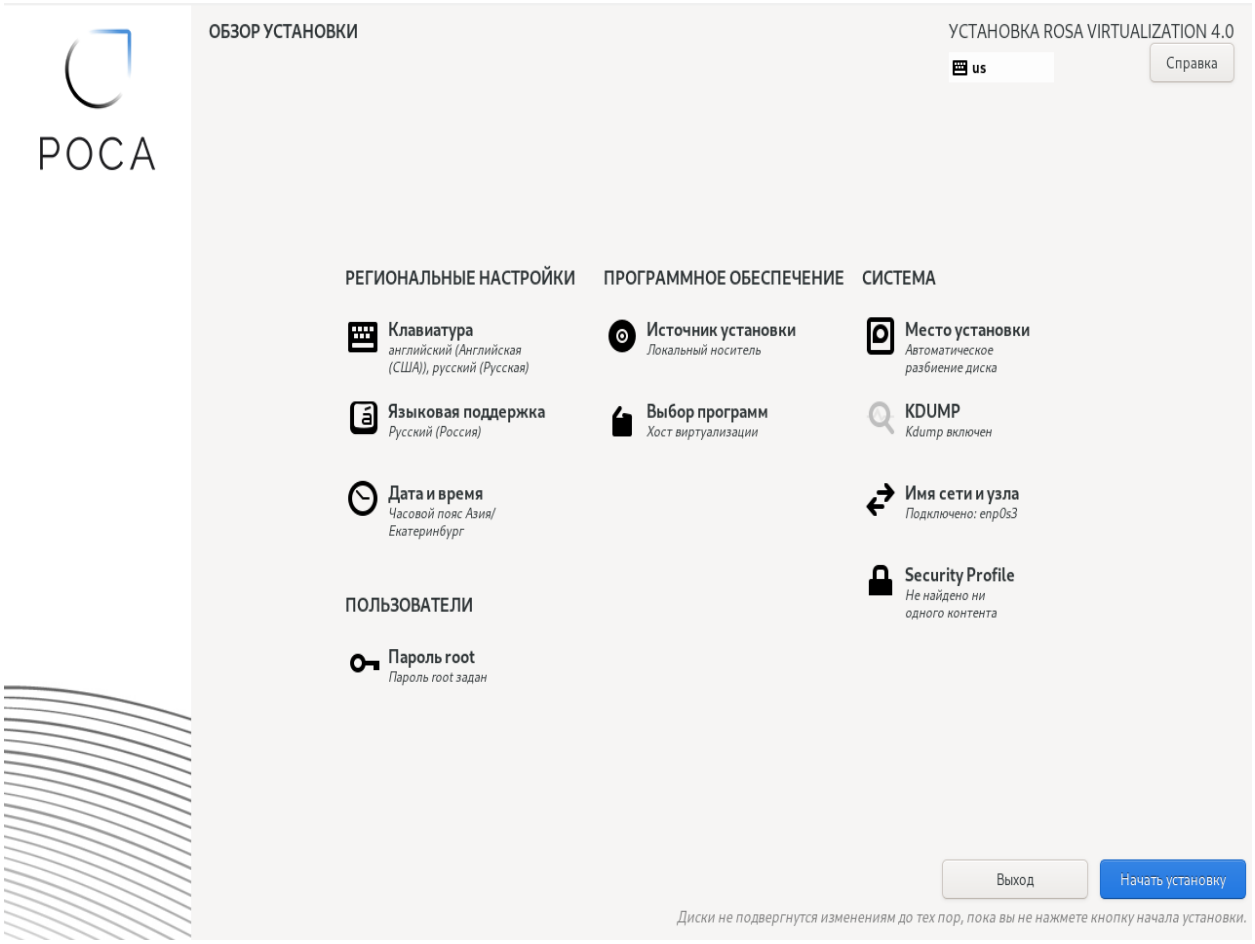

Рисунок 23 – Обзор установки

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

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

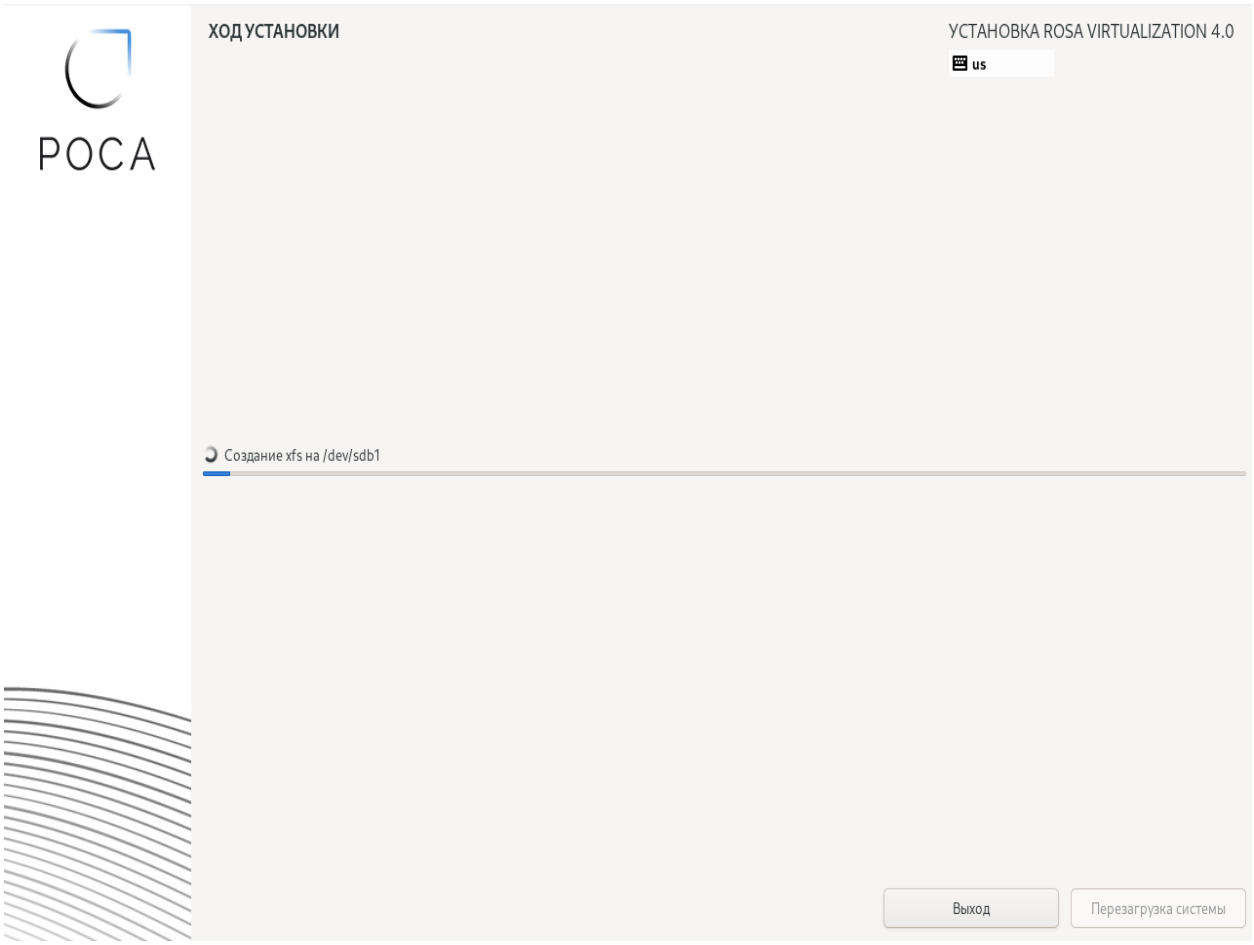

Рисунок 24 – Процесс установки РОСА Виртуализация

3.2.6 Завершение установки

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

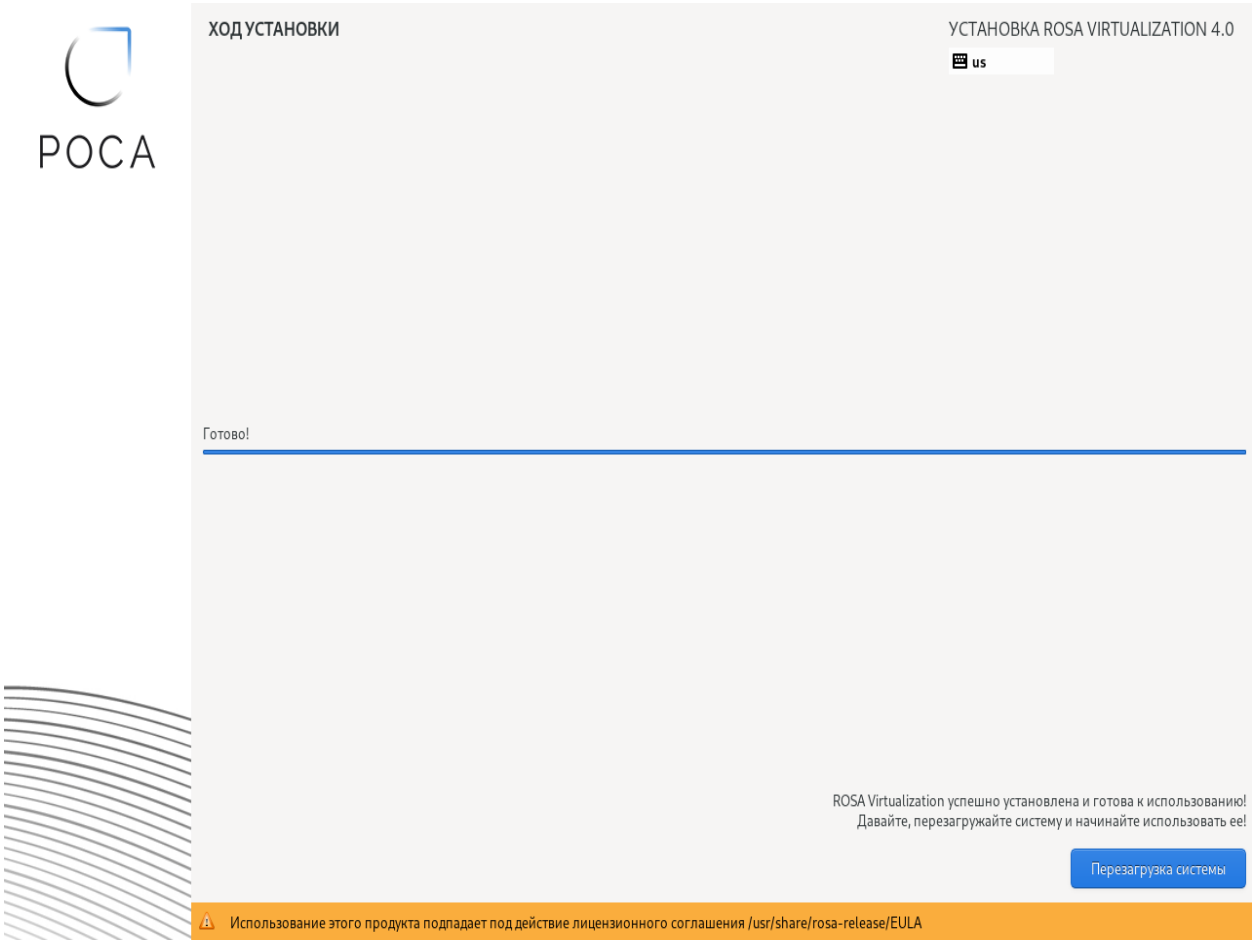

Рисунок 25 – Завершение процесса установки

Далее следует извлечь DVD- или USB-накопитель, с которого выполнялась установка.

После перезагрузки системы, в случае если управляющая сеть ovirtmgmt должна быть тегированной изначально, необходимо:

а) убедиться, что на вышестоящем коммутаторе созданы соответствующие VLAN и порт настроен для транкинга;

б) на хосте гипервизора переименовать (в случае отсутствия — создать с нужным именем) конфигурационный файл физического интерфейса ifcfg-physical_device в папке /etc/sysconfig/network-scripts/ к виду ifcfg-physical_device.vlanID, где:

– physical_device — имя физического интерфейса;
– vlanID — номер VLAN.

Например, для физического интерфейса eth0 и VLAN ID с номером 17 новое имя файла будет таким:/etc/sysconfig/network-scripts/ifcfg-eth0.17.

в) настроить конфигурационный файл, для чего указать параметры:

– ONBOOT — загрузка интерфейса при старте системы — "yes";
– TYPE — тип интерфейса — "Vlan";
– PHYSDEV — имя физического интерфейса;
– VLAN — включение интерфейса как VLAN — "yes";
– VLAN_ID — номер VLAN;
– VLAN_NAME_TYPE — тип именования VLAN-интерфейса — "VLAN_NAME_TYPE_RAW_PLUS_VID_NO_PAD";
– DEVICE — имя сабинтерфейса с указанием родительского интерфейса и VLAN ID;
– BOOTPROTO — метод загрузки (статический или DHCP) — "static";
– IPADDR — статический IP-адрес интерфейса;
– NETMASK — маска подсети;
– GATEWAY — IP-адрес шлюза;
– DNS1 — IP-адрес DNS.

Например:

```
ONBOOT=yes
TYPE=Vlan
PHYSDEV=eth0
VLAN=yes
DEVICE=eth0.17
VLAN_ID=17
VLAN_NAME_TYPE=VLAN_NAME_TYPE_RAW_PLUS_VID_NO_PAD
BOOTPROTO=static
IPADDR=192.168.0.15
NETMASK=255.255.255.0
GATEWAY=192.168.0.1
DNS1=192.168.0.2
DNS2=192.168.0.3
```

г) перезапустить службу сети, чтобы изменения вступили в силу, для чего выполнить команду:

```
systemctl restart NetworkManager.service
```

На этом установка хоста завершена, и нужно выполнить вход в веб-интерфейс администрирования хоста гипервизора для продолжения настройки и установки компонентов РОСА Виртуализация.

Важно – Для развертывания РОСА Виртуализация в базовой конфигурации необходимо установить как минимум 3 гипервизора на различных хостах.

3.2.7 Вход в веб-интерфейс хоста гипервизора

Для доступа к веб-интерфейсу хоста гипервизора нужно ввести 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 нужно нажать 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 необходимо осуществить вход в интерфейс от имени учетной записи суперпользователя root, используя пароль, выбранный ранее (см. п. Ошибка: источник перекрёстной ссылки не найден).

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

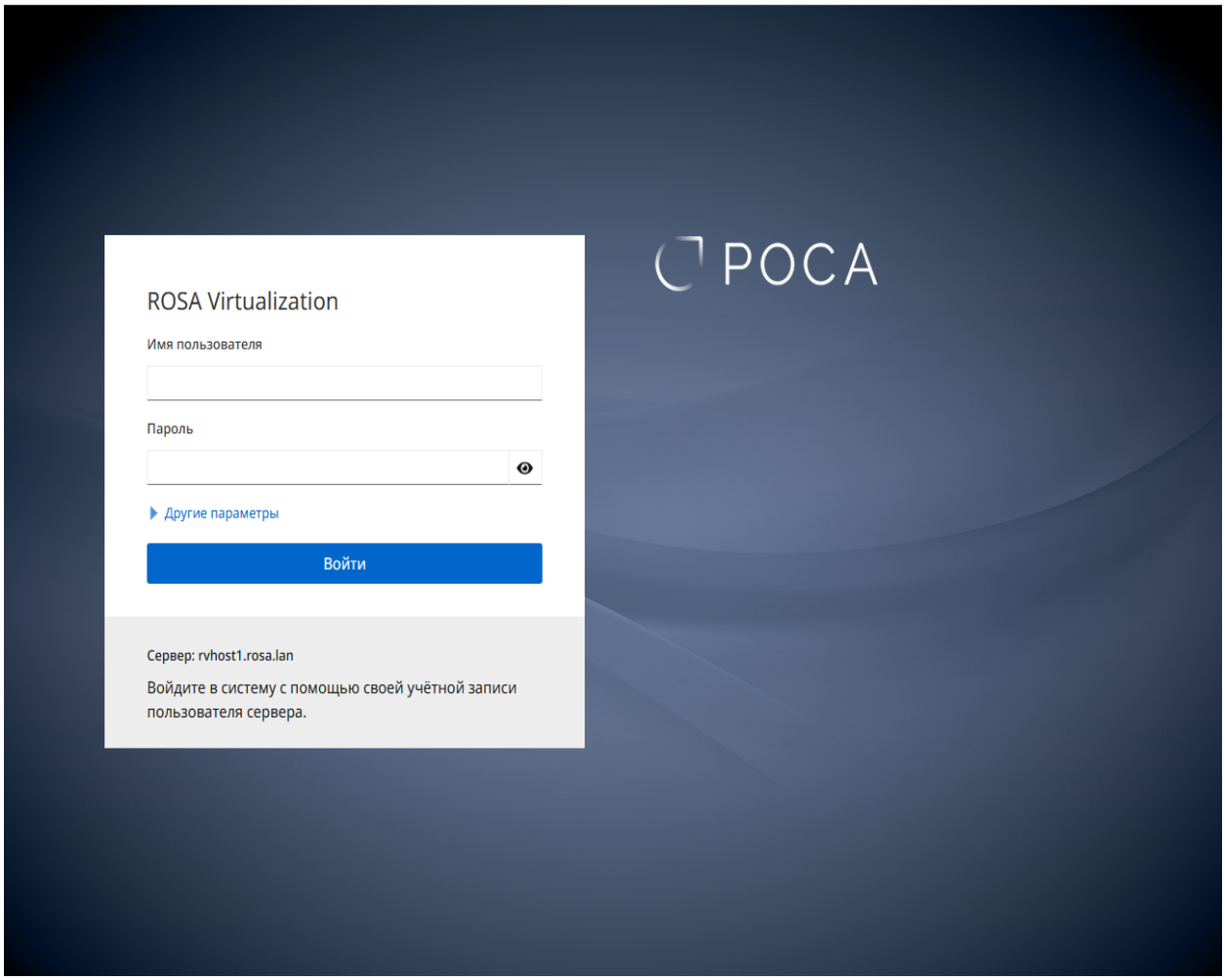

Рисунок 26 – Окно авторизации веб-интерфейса хоста гипервизора

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 можно использовать необходимые вкладки панели навигации.

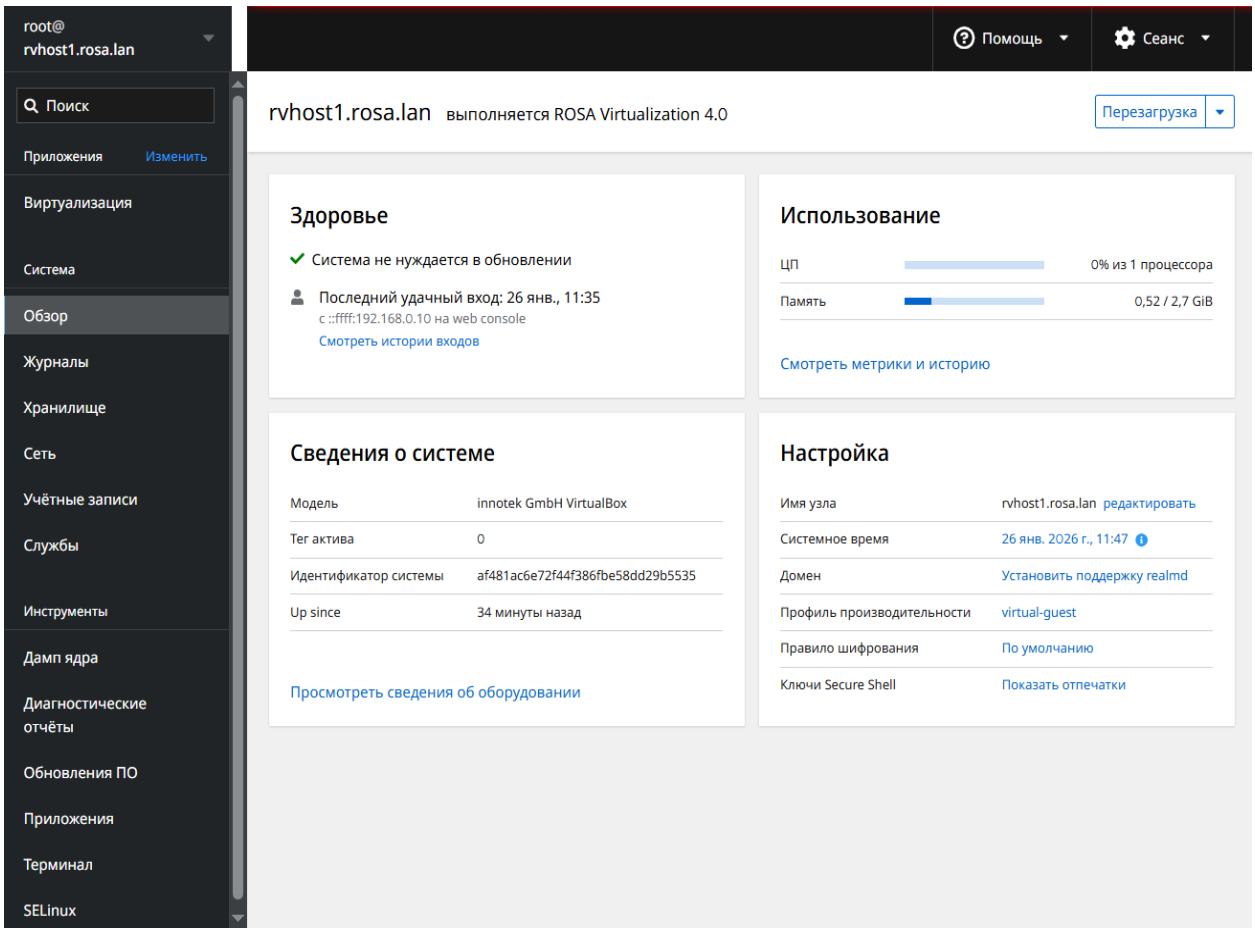

Рисунок 27 – Интерфейс хоста гипервизора (Панель навигации, секции "Здоровье", "Использование", "Сведения о системе", "Настройка")

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 нужно перейти на вкладку "Терминал" панели навигации интерфейса соответствующего хоста гипервизора (рисунок 28).

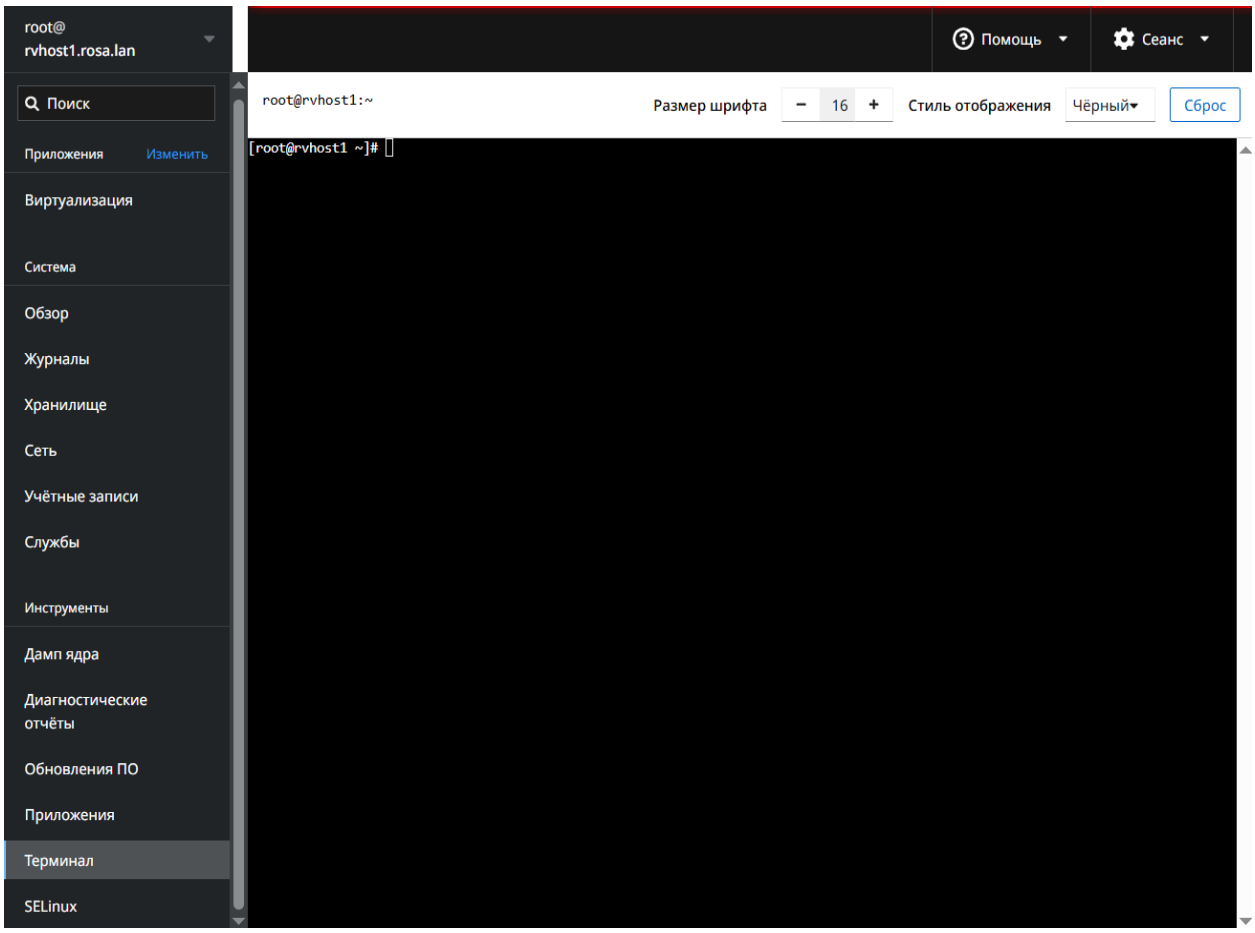

Рисунок 28 – Консоль (терминал) хоста гипервизора, с доступом через веб-интерфейс

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 используют имя учетной записи суперпользователя root и пароль, выбранный ранее (см. п.Ошибка: источник перекрёстной ссылки не найден).

В терминале необходимо выполнить следующую команду, указав имя хоста, развернутого в актуальном ЦОД вместо rvhost1.rosa.lan:

```
# 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 веб-интерфейсе администрирования хоста.

3.3.3 Разрешение имен DNS

При отсутствии в сети сервера DNS используют 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

Для редактирования в консоли хоста нужно открыть редактор mcedit и указать в файле /etc/hosts IP-адреса и имена DNS взаимодействующих компонентов РОСА Виртуализация – хостов с установленными гипервизорами, ВМ СУСВ и сервера IPA – с помощью следующей команды в консоли:

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

После завершения редактирования следует выйти из редактора, сохранив результат. Для выхода из редактора можно использовать кнопку `Esc`. Если в файл были внесены изменения, то будет предложено сохранить их или выйти без сохранения. Для сохранения внесенных изменений требуется выбрать опцию "Сохранить при выходе" – "Да" при выходе из редактора.

Примечания:

1) Для сохранения результатов редактирования файла в редакторе mcedit нажать `F2`. Для выхода из редактора нажать `F10`. При использовании редактора в окне браузера можно 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 выполняют команду:

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

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

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

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

Пример файла /etc/hosts с IP-адресами и именами DNS взаимодействующих компонентов РОСА Виртуализация – 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
```

Процедуру редактирования файла /etc/hosts следует повторить на каждом из хостов с установленным гипервизором.

Примечания:

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

2) Указание в файле /etc/hosts IP-адресов и имен DNS взаимодействующих компонентов РОСА Виртуализация 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 создают на каждом хосте закрытый и открытый ключи SSH, а затем копируют открытый ключ на другие хосты.

3.3.4.1 Создание ключей SSH

Для создания ключей SSH нужно выполнить следующую консольную команду:

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

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

3.3.4.2 Копирование открытых криптографических ключей на другие хосты

После создания ключей нужно скопировать открытый ключ на другие хосты, для чего выполнить следующую команду, последовательно указывая имена всех необходимых хостов:

```
# ssh-copy-id имя_хоста
```

В качестве "имя_хоста" в команде выше необходимо указать 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 нужно выполнить 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.
```

Следует повторить 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 РОСА Виртуализация 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 средства виртуализации необходимо создать файловое хранилище или использовать уже имеющееся хранилище.

Для создания файлового хранилища NFS на основе хоста гипервизора нужно выполнить следующие действия:

а) открыть в панели управления секцию "Виртуализация" (рисунок 29);

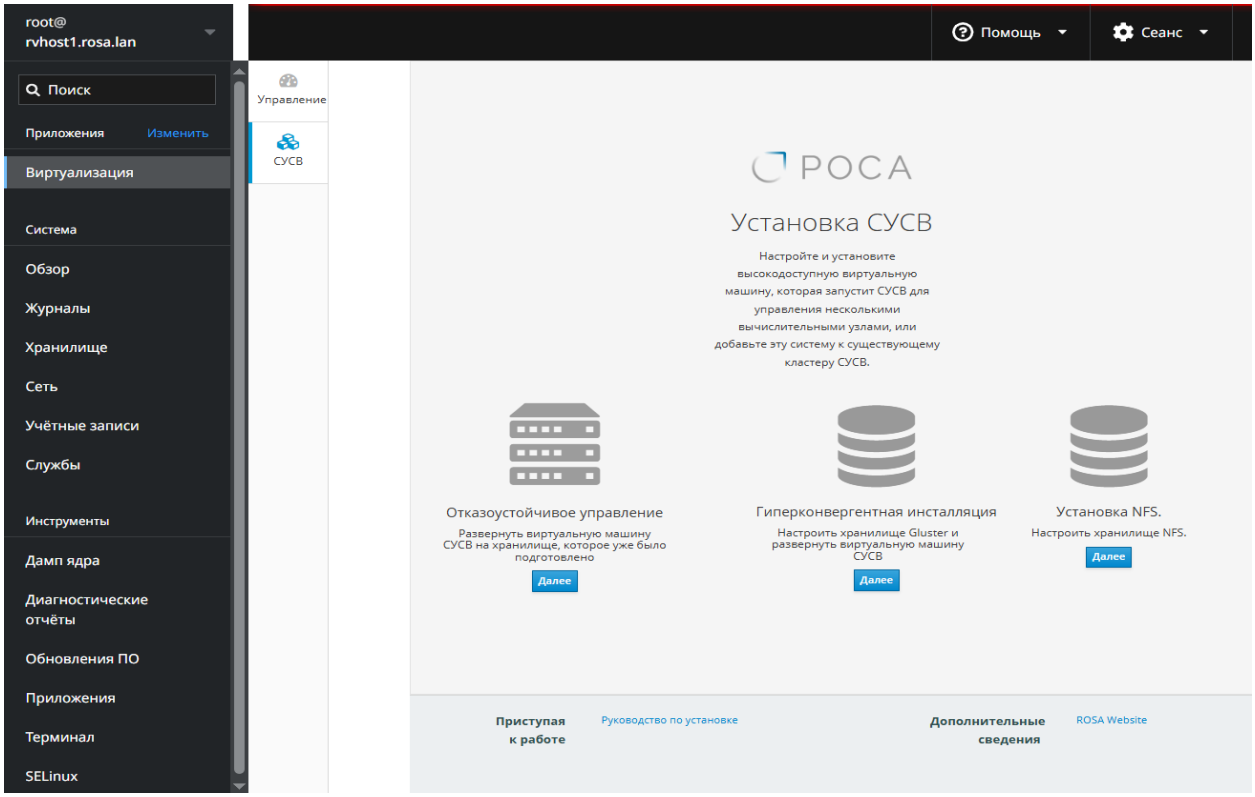

Рисунок 29 – Интерфейс модуля установки СУСВ и настройки файлового хранилища

б) выбрать в интерфейсе секцию "Установка NFS" и нажать на кнопку Далее. В результате откроется диалоговое окно для настройки файлового хранилища NFS (рисунок 30);

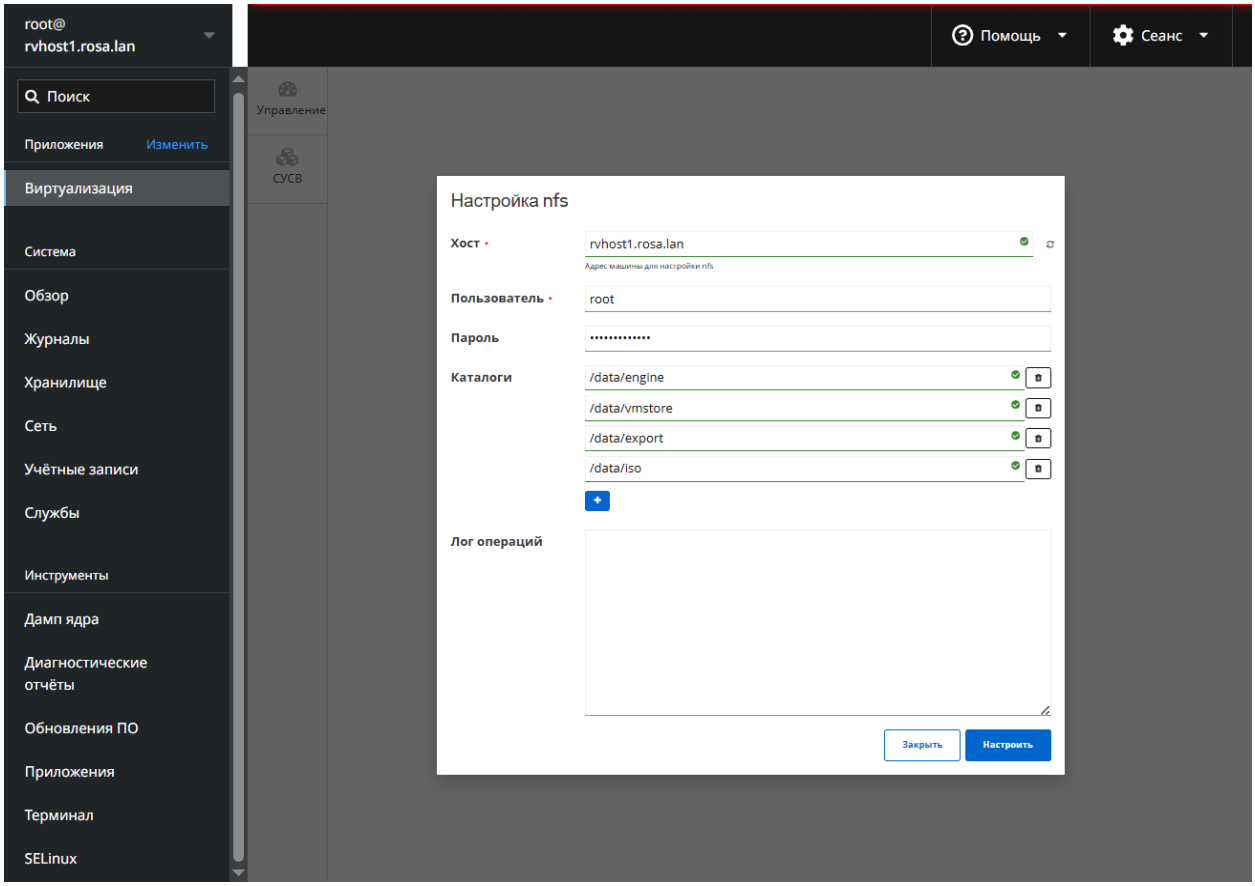

Рисунок 30 – Интерфейс окна для настройки хранилища NFS

в) для настройки хранилища NFS потребуются имя хоста, имя и пароль пользователя, имеющего права суперпользователя, и структура каталогов (предлагается использовать структуру по умолчанию) (рисунок 31). После ввода требуемых параметров запустить процесс (кнопка Настроить), хранилище NFS будет создано и настроено, в форму "Лог операций" будет выведен лог выполненных действий;

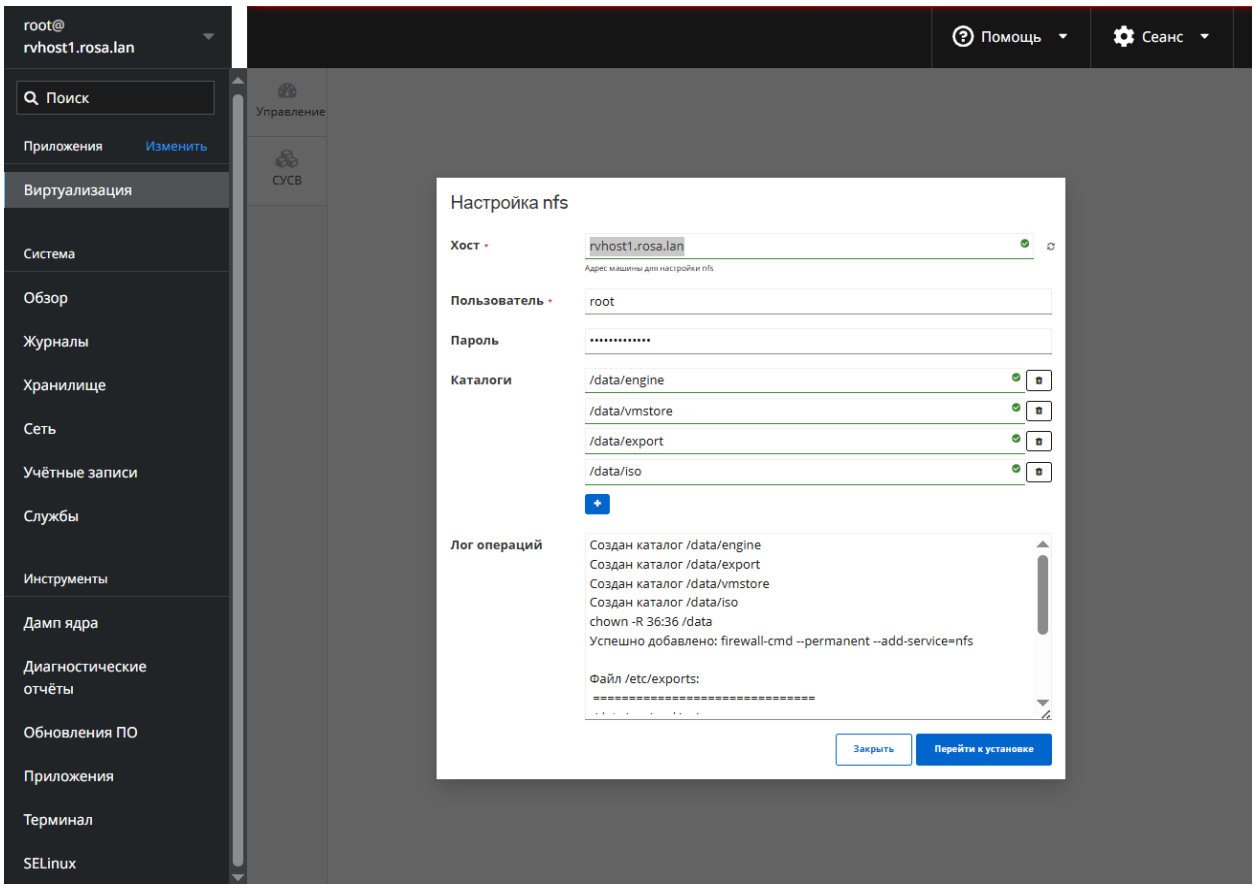

Рисунок 31 – Интерфейс окна для настройки хранилища NFS с указанным именем хоста, логином и лог выполненных действий

г) 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 можно проверить работоспособность хранилища NFS, выполнив в консоли хоста команду:

```
    # systemctl status nfs-server
    ●  Loaded: loaded (/usr/lib/systemd/system/nfs-
server.service; enabled; preset: disabled)
        Drop-In: /run/systemd/generator/nfs-server.service.d
                 └─order-with-mounts.conf
         Active: active (exited) since Mon 2026-01-26 14:59:26
+05; 8min ago
           Docs: man:rpc.nfsd(8)
```

```
                  man:exportfs(8)
         Process: 984 ExecStartPre=/usr/sbin/exportfs -r
(code=exited, status=0/SUCCESS)
         Process: 988 ExecStart=/usr/sbin/rpc.nfsd (code=exited,
status=0/SUCCESS)
         Process: 1072 ExecStart=/bin/sh -c if systemctl -q is-
active gssproxy; then systemctl reload gssproxy ; fi
(code=exited, stat>
        Main PID: 1072 (code=exited, status=0/SUCCESS)
             CPU: 137ms

     янв 26 14:59:23 rvhost1.rosa.lan systemd[1]: Starting NFS
server and services...
     янв 26 14:59:26 rvhost1.rosa.lan systemd[1]: Finished 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 РОСА Виртуализация в консоли хоста, предназначенного для установки ВМ СУСВ.

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

Для доступа к консоли нужно перейти на вкладку "Терминал" панели навигации интерфейса соответствующего хоста или открыть 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, нужно создать определенную структуру каталогов. Для создания каталогов используют редактор mc или консольную утилиту mkdir.

Например, можно выполнить следующую команду:

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

Для изменения владельца всех созданных каталогов на служебного пользователя vdsm (uid=36) и соответствующую служебную группу kvm (gid=36) требуется выполнить следующую команду:

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

В редакторе mc (запуск редактора осуществляется из командной строки терминала командой `mcedit`) следует отредактировать конфигурационный файл сервера NFS /etc/exports так, чтобы предоставить всем хостам в сети доступ к созданным каталогам на чтение и запись. Для этого нужно добавить 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 нужно выполнить следующую команду:

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

Для применения изменений следует перезагрузить конфигурацию межсетевого экрана, для чего выполнить 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 нужно выполнить 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, выполняют следующую команду:

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

3.4.2.3.1 Проверка работоспособности NFS-сервера

Для проверки статуса NFS-сервера выполняют 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 необходимо перейти 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.

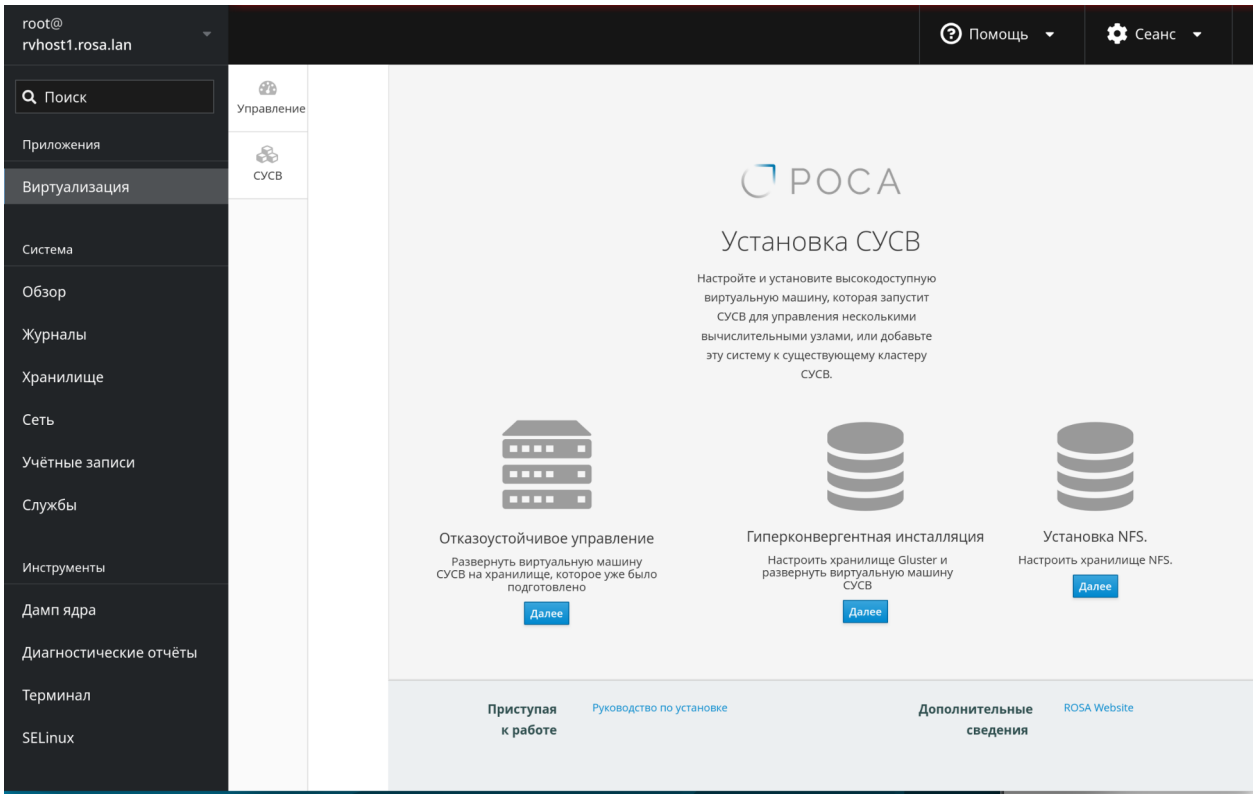

Рисунок 32 – Выбор варианта установки СУСВ в веб-интерфейсе хоста виртуализации

Выбор варианта установки СУСВ:

– Для установки СУСВ на заранее подготовленное хранилище нужно нажать 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 нужно нажать кнопку Далее в секции "Гиперконвергентная инсталляция". Программа установки запустит интерактивный процесс развертывания хранилища Gluster (см. п. 3.5.1).

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

3.5.1 Развертывание хранилища Gluster

Для развертывания и настройки хранилища Gluster для группы из трёх хостов нужно выполнить следующие действия:

а) в окне "Конфигурация Gluster" нажать кнопку Запустить установщик Gluster для перехода к настройке конфигурации хранилища (рисунок 33);

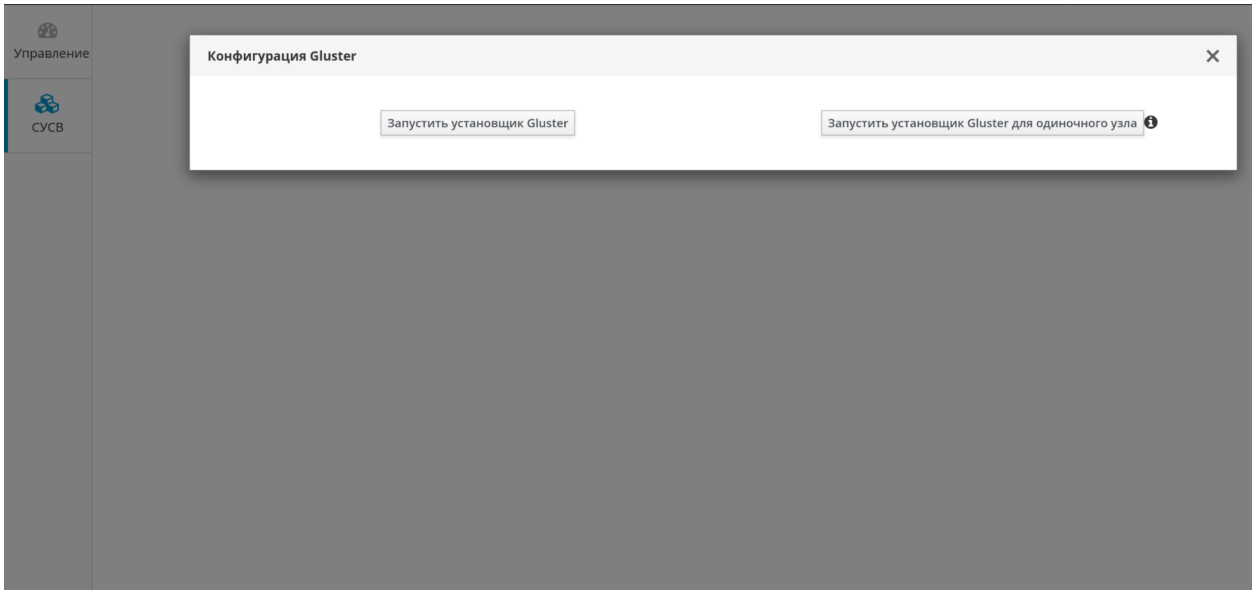

Рисунок 33 – Запуск настройки конфигурации Gluster

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

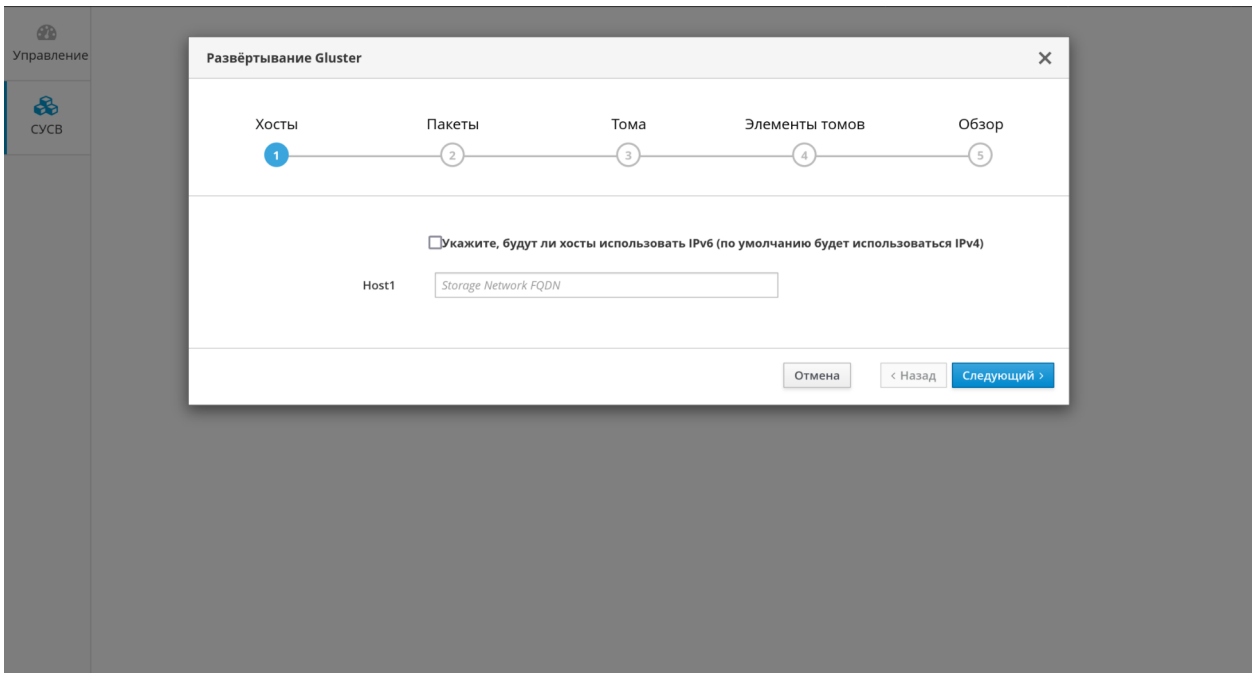

Рисунок 34 – Форма помощника настройки конфигурации Gluster для одиночного узла

б) 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);

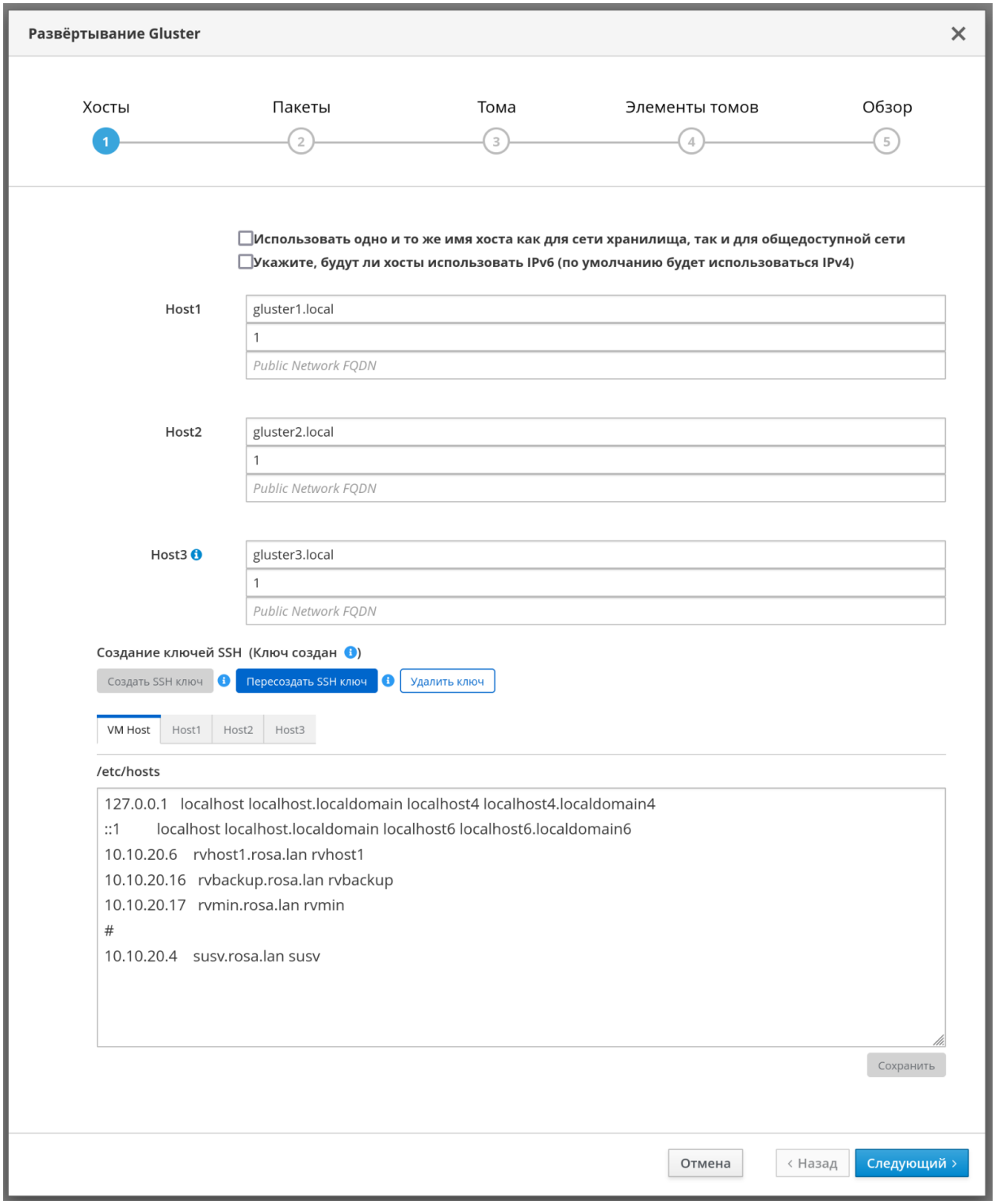

Рисунок 35 – Форма помощника настройки конфигурации Gluster для группы из трех хостов – секция "Параметры хостов"

в) в секции "Хосты" ввести полные доменные имена развернутых хостов РОСА Виртуализация в соответствующие поля, при этом хост, указанный в поле

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

г) если указанные имена хостов будут использоваться как для сети хранилища, так и для общедоступной сети, установить соответствующий флажок или отдельно ввести имена хостов для общедоступной сети в нижней строке каждого поля;

д) для продолжения настройки конфигурации хранилища нажать кнопку Следующий для перехода к секции "Пакеты" (рисунок 36);

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

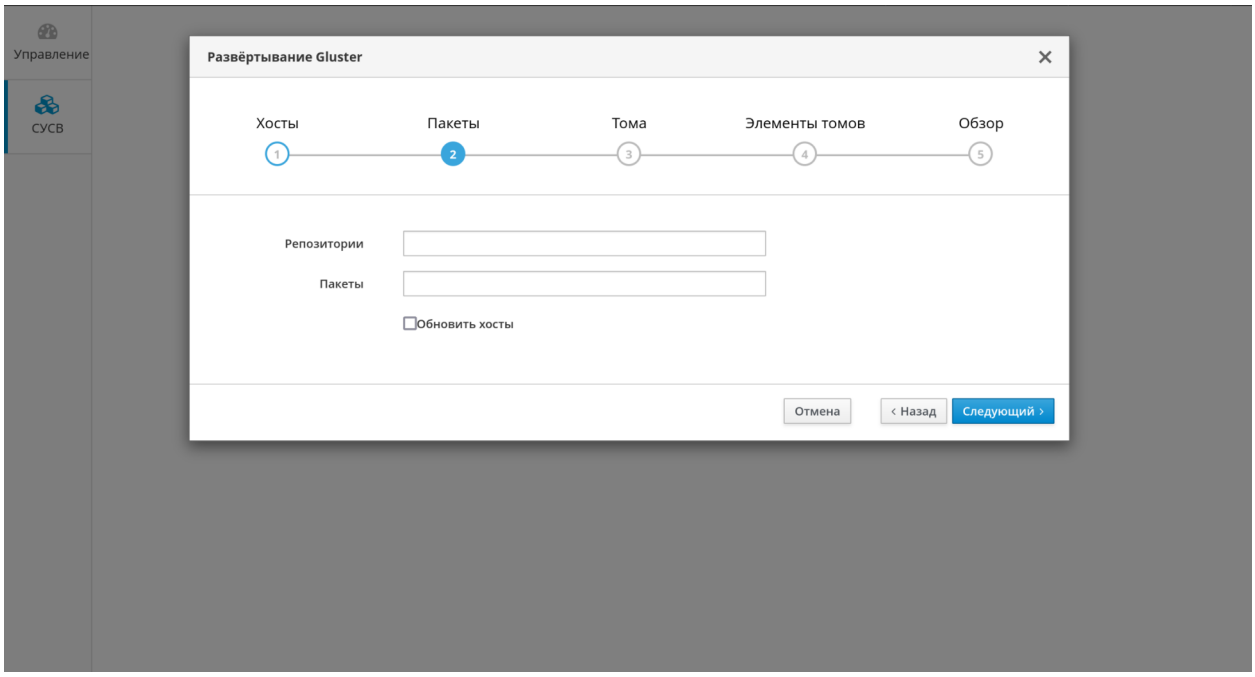

Рисунок 36 – Помощник настройки конфигурации Gluster – секция "Пакеты"

е) в секции "Пакеты" нажать кнопку Следующий для продолжения настройки конфигурации хранилища и перехода к секции "Тома" (рисунок 37);

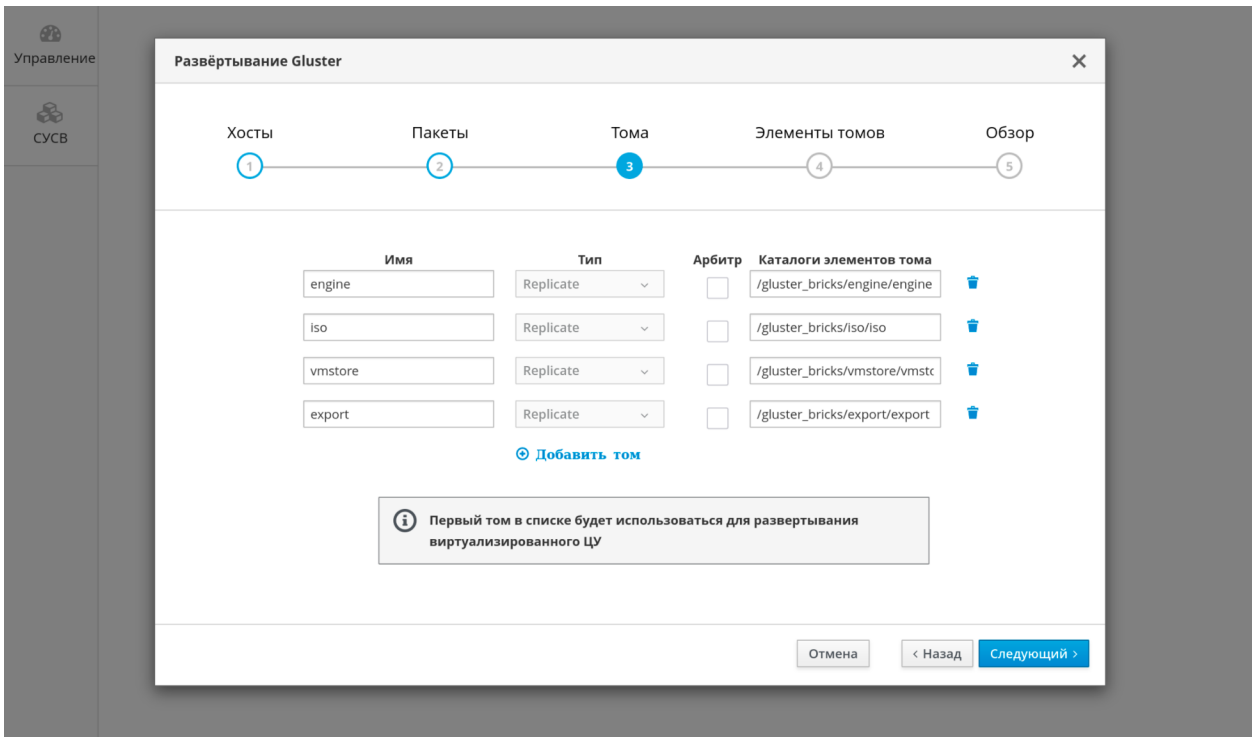

Рисунок 37 – Параметры томов Gluster

ж) в секции "Тома" изменить имя тома "data" на значение "iso" и добавить новый том "export";

з) для добавления нового тома нажать на функциональную строку Добавить том и в поле "Имя" с параметрами нового тома ввести 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.

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

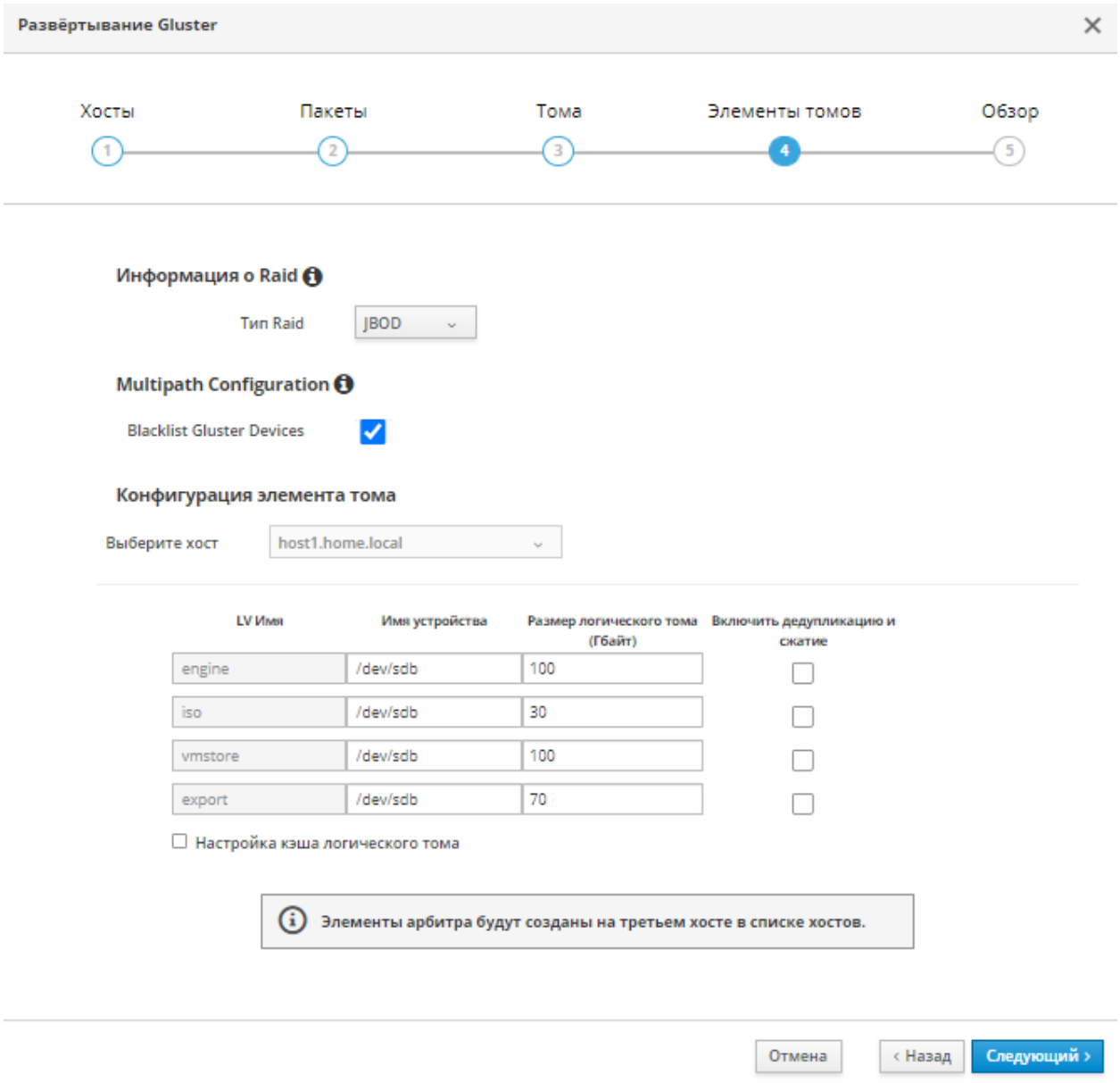

Рисунок 38 – Конфигурация элементов томов Gluster

к) в секции "Элементы томов" из выпадающего списка "Тип Raid" выбрать значение "JBOD", а также при необходимости отредактировать значения конфигурации элемента для каждого тома;

л) в графе "Имя устройства" указать дисковый накопитель (по умолчанию /dev/sdb), предназначенный для развертывания хранилища;

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

м) в графе "Размер логического тома (Гбайт)" указать 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.

н) нажать кнопку Следующий для перехода к секции "Обзор" (рисунок 39);

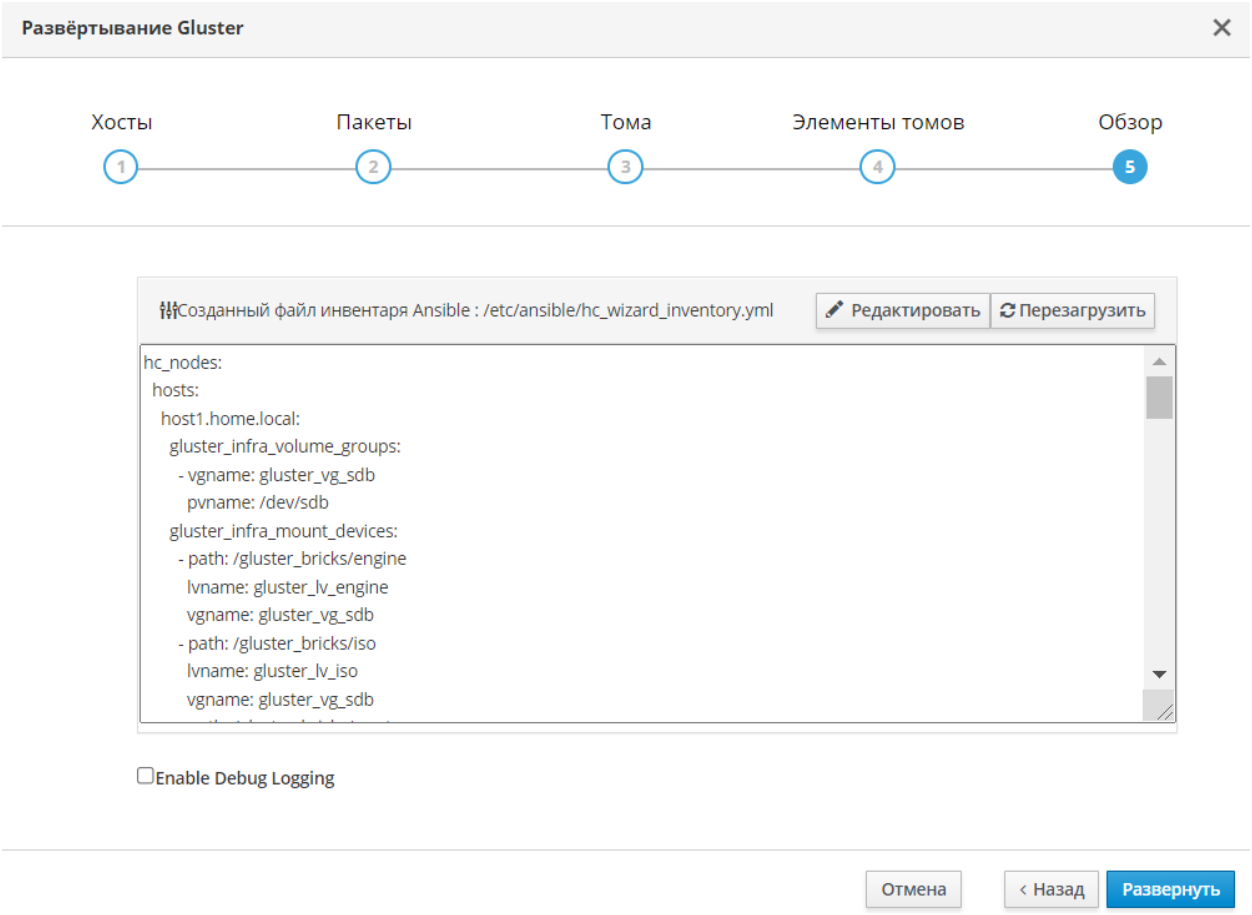

Рисунок 39 – Обзор параметров конфигурации хранилища Gluster

о) в секции "Обзор" нажать 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.

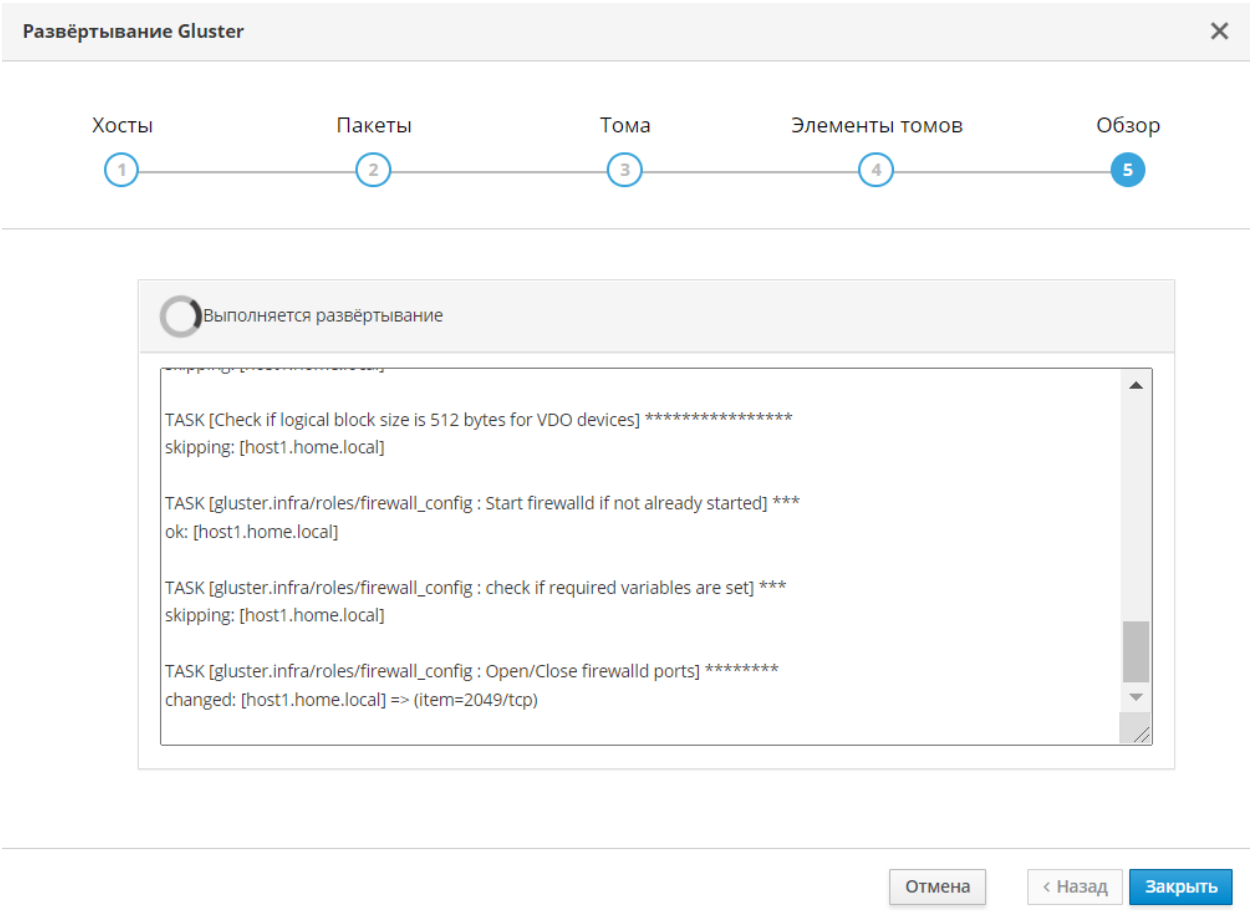

Рисунок 40 – Ход процесса развертывания хранилища Gluster

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

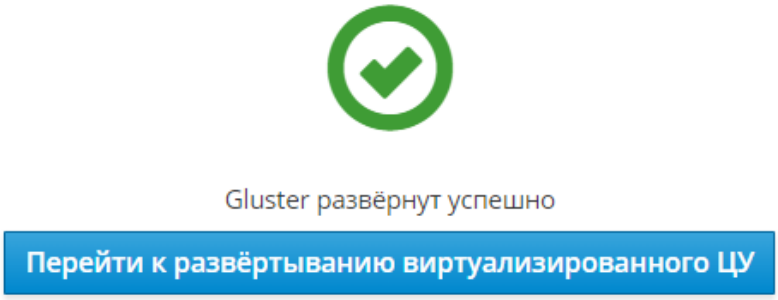

Рисунок 41 – Завершение развертывания хранилища Gluster

Для запуска интерактивного процесса установки ВМ СУСВ на развернутое хранилище Gluster необходимо нажать 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).

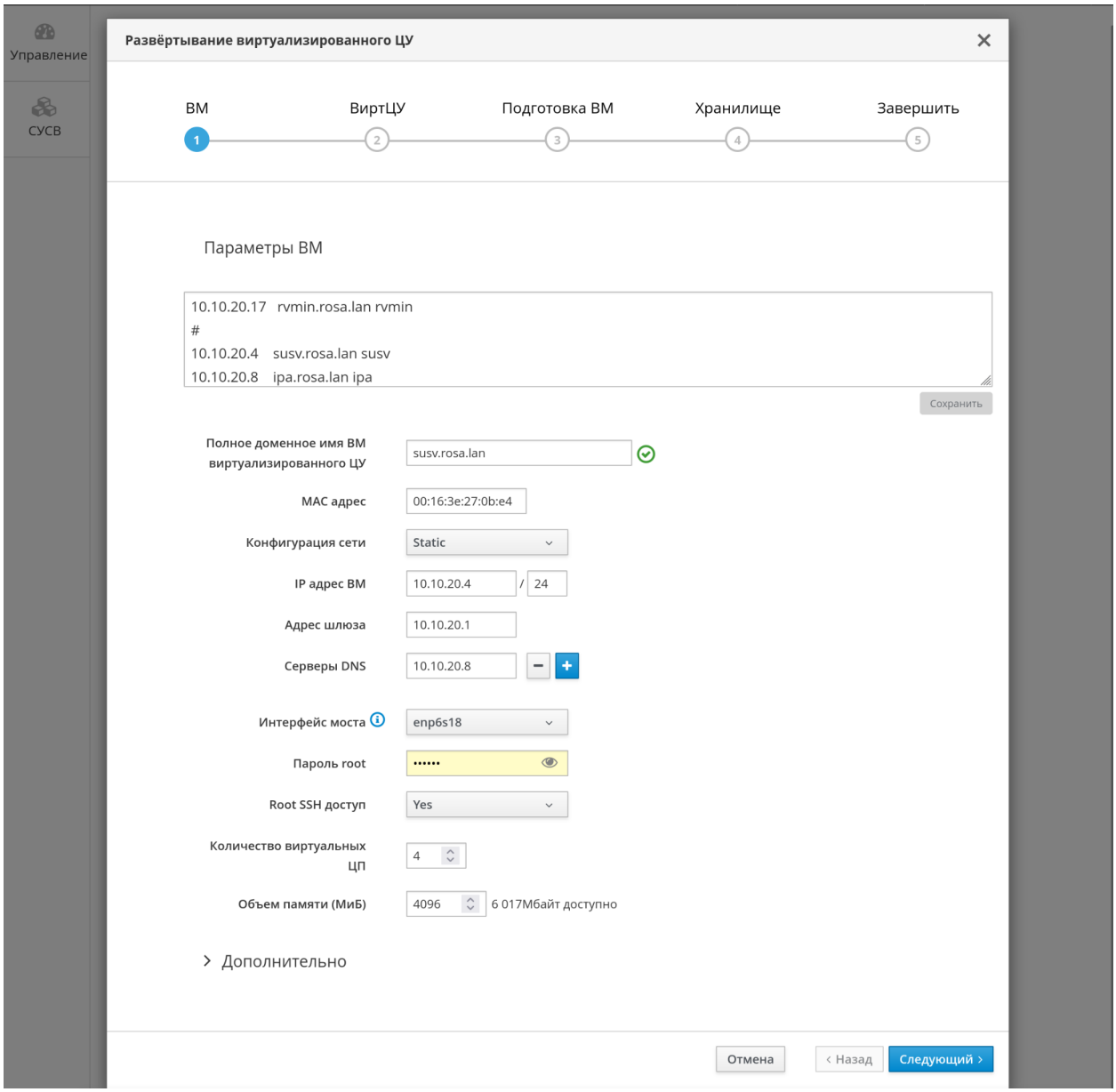

Рисунок 42 – Задание параметров ВМ для развертывания виртуализированного ЦУ

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.

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.

В поле, соответствующем файлу /etc/hosts, нужно указать IP-адреса и имена DNS взаимодействующих компонентов РОСА Виртуализация – хостов с установленными гипервизорами, ВМ СУСВ и сервера IPA.

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

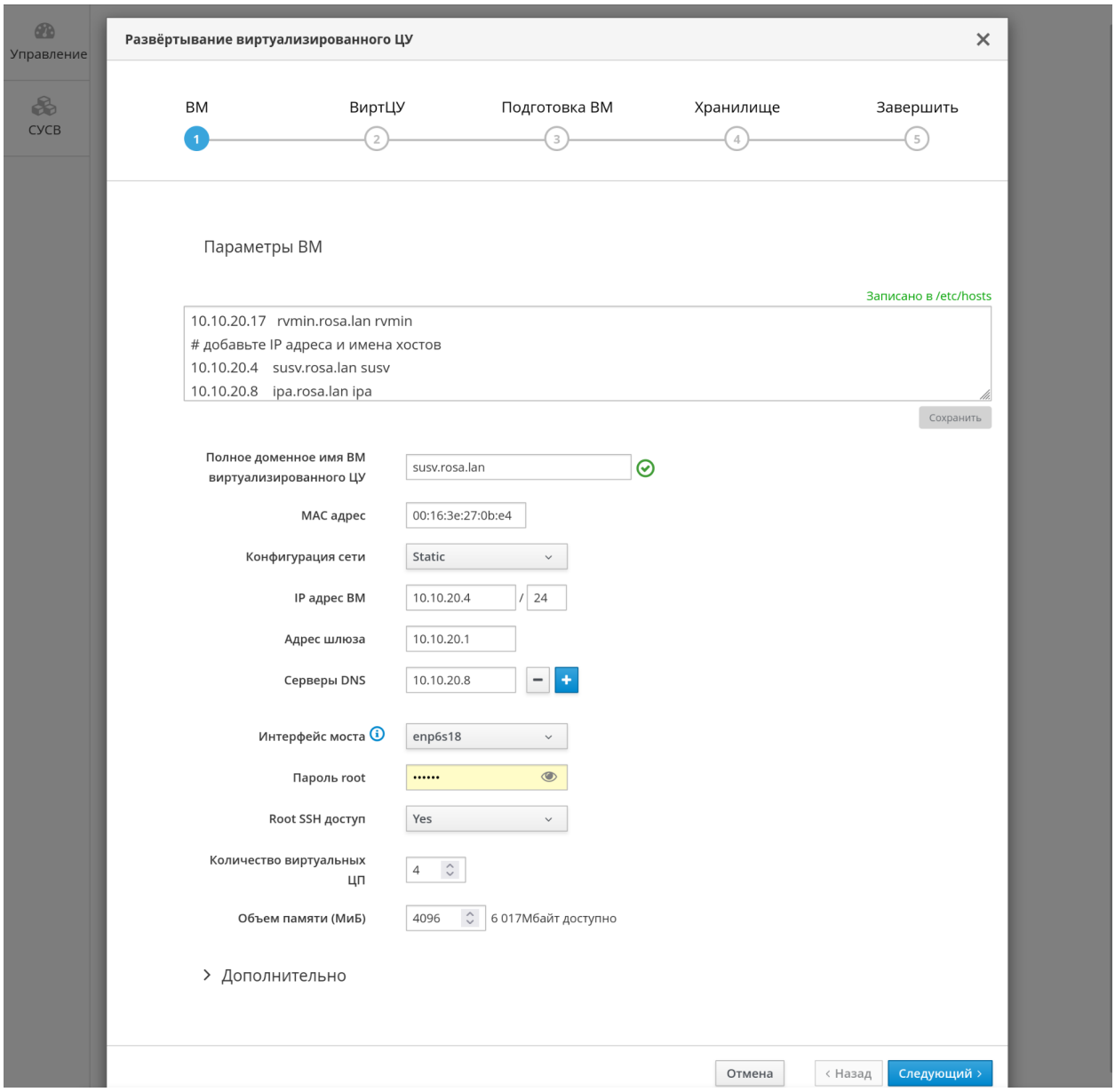

Рисунок 43 – Сохранение содержимого формы в файл /etc/hosts

В поле "Полное доменное имя ВМ виртуализированного ЦУ" нужно задать полное доменное имя ВМ СУСВ (например, "susv.rosa.lan").

Примечание – Доменное имя ВМ СУСВ должно быть разрешено 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 необходимо предпринять дополнительные шаги для обеспечения разрешения доменного имени.

Далее из выпадающего списка "Конфигурация сети" следует выбрать необходимое значение – "DHCP" или "Static".

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

Затем при выборе в конфигурации сети значения "Static" нужно указать 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 следует нажать кнопку + и ввести IP-адрес в новом поле);

– Пароль root – пароль для учетной записи суперпользователя root ВМ СУСВ;

– Root SSH доступ" – "Yes".

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

При указании значения объема оперативной памяти в соответствующем поле следует учитывать, что при развертывании РОСА Виртуализация 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"

Для настройки (при необходимости) дополнительных параметров установки нужно нажать на секцию "Дополнительно" (рисунок 44) и заполнить поля:

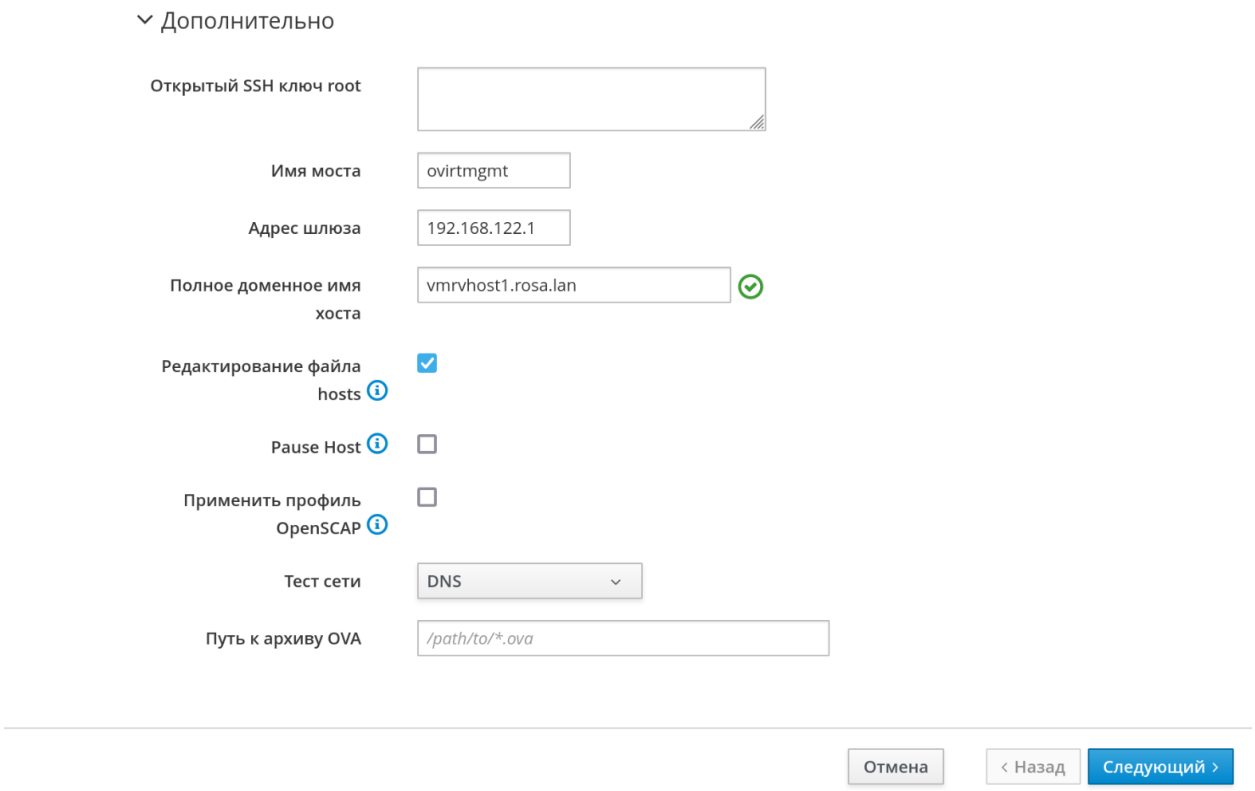

Рисунок 44 – Настройка дополнительных параметров

– 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 разрешено;

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

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

– Pause Host – отметить эту опцию, если требуется 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 – выбрать способ тестирования сети. При выборе опции "none" тестирование сети осуществляться не будет:

– DNS;
– Ping;
– TCP;
– None;

– 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.

Затем нужно нажать кнопку Следующий для продолжения настройки конфигурации СУСВ и перехода к секции "ВиртЦУ".

3.5.2.2 Настройка виртуализированного ЦУ

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

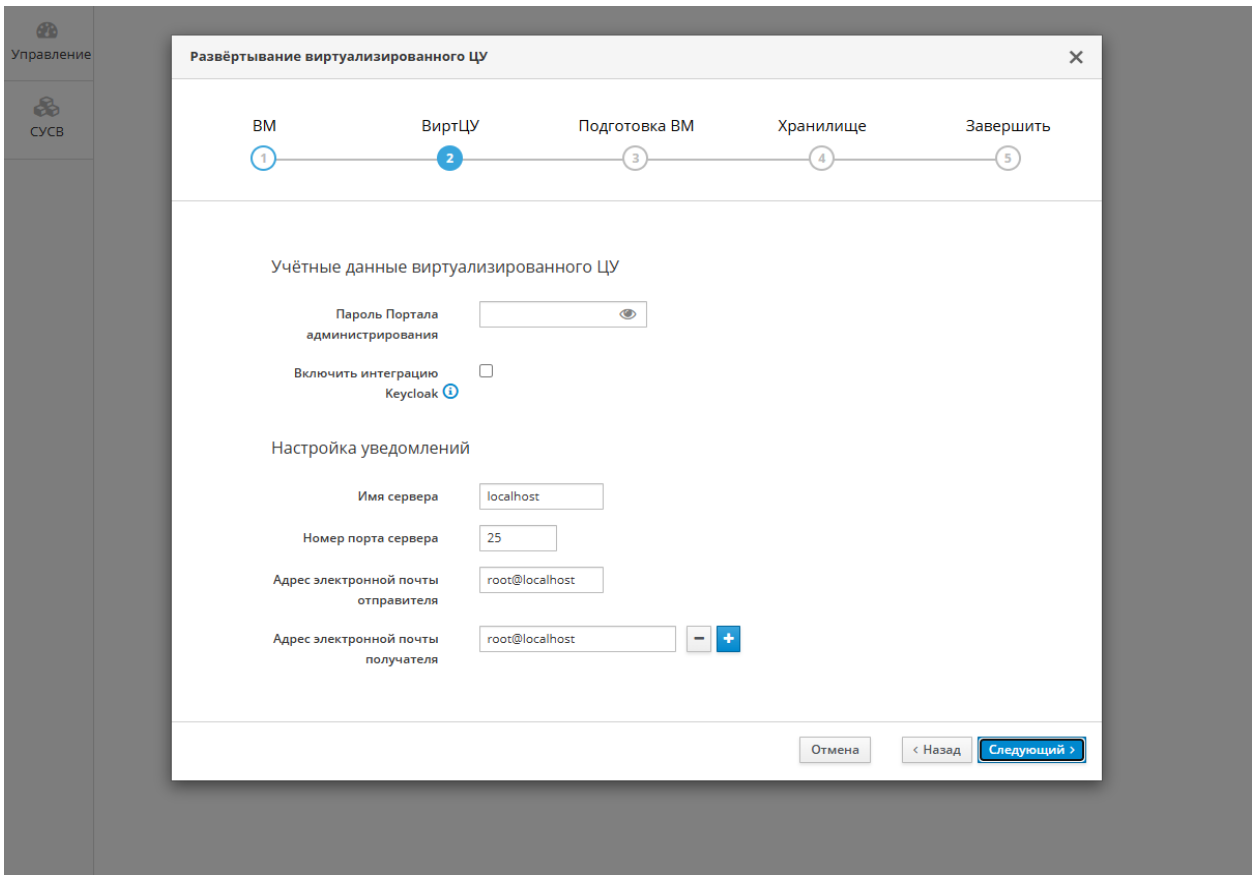

Рисунок 45 – Параметры СУСВ (Виртуального ЦУ)

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

Затем нужно нажать кнопку `Следующий` для перехода к секции "Подготовка ВМ".

3.5.2.3 Подготовка виртуальной машины

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

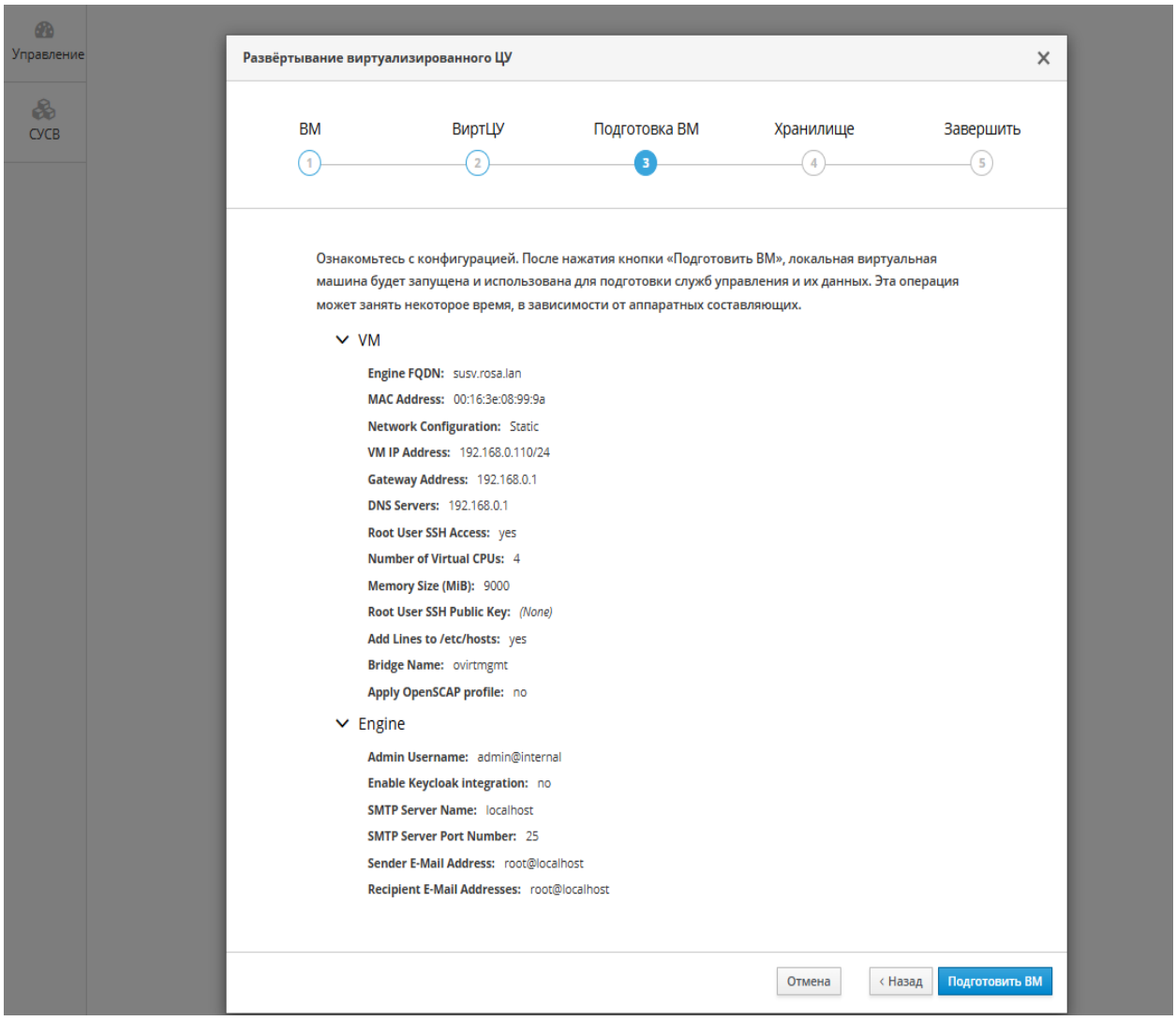

Рисунок 46 – Обзор параметров конфигурации ВМ Виртуального ЦУ (СУСВ)

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

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

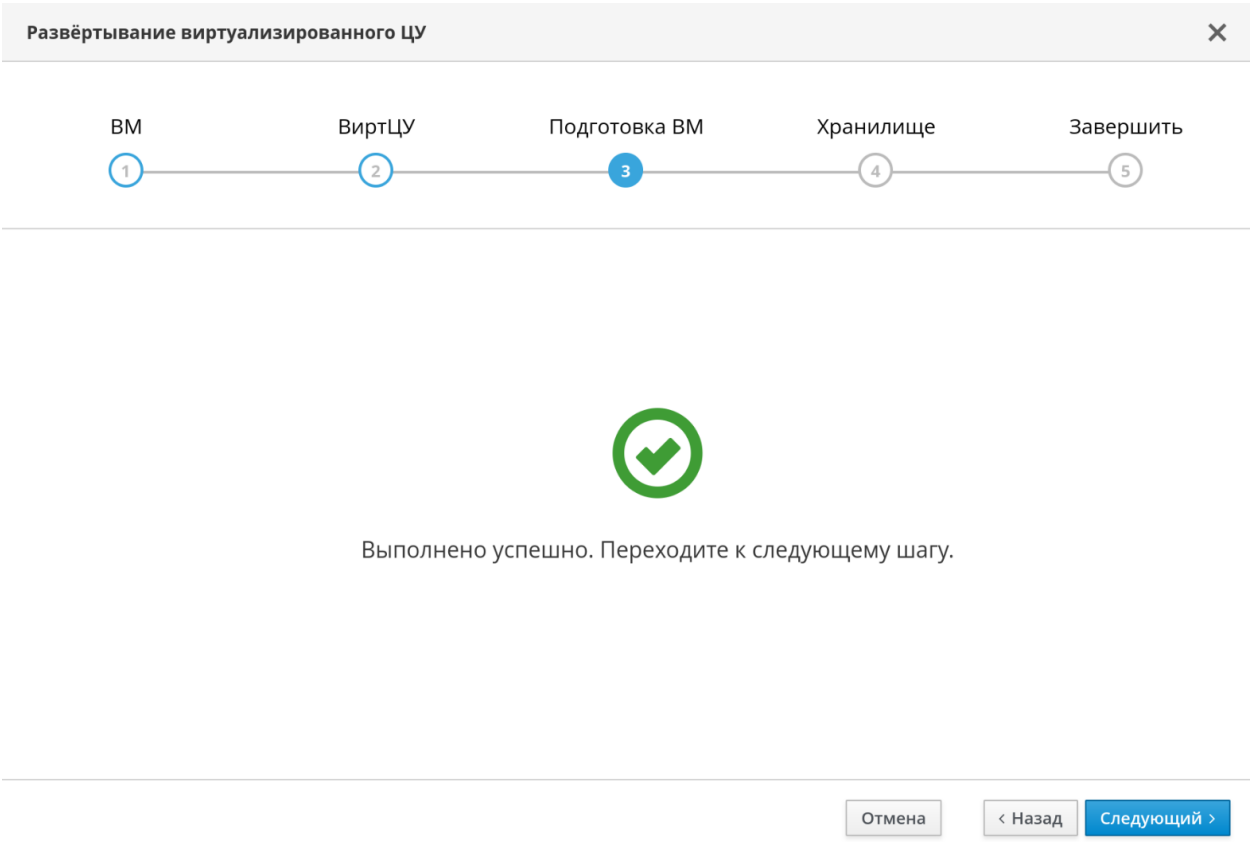

Рисунок 47 – Завершение подготовки ВМ

Затем нужно нажать кнопку Следующий для перехода к секции "Хранилище".

3.5.2.4 Настройка параметров хранилища

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

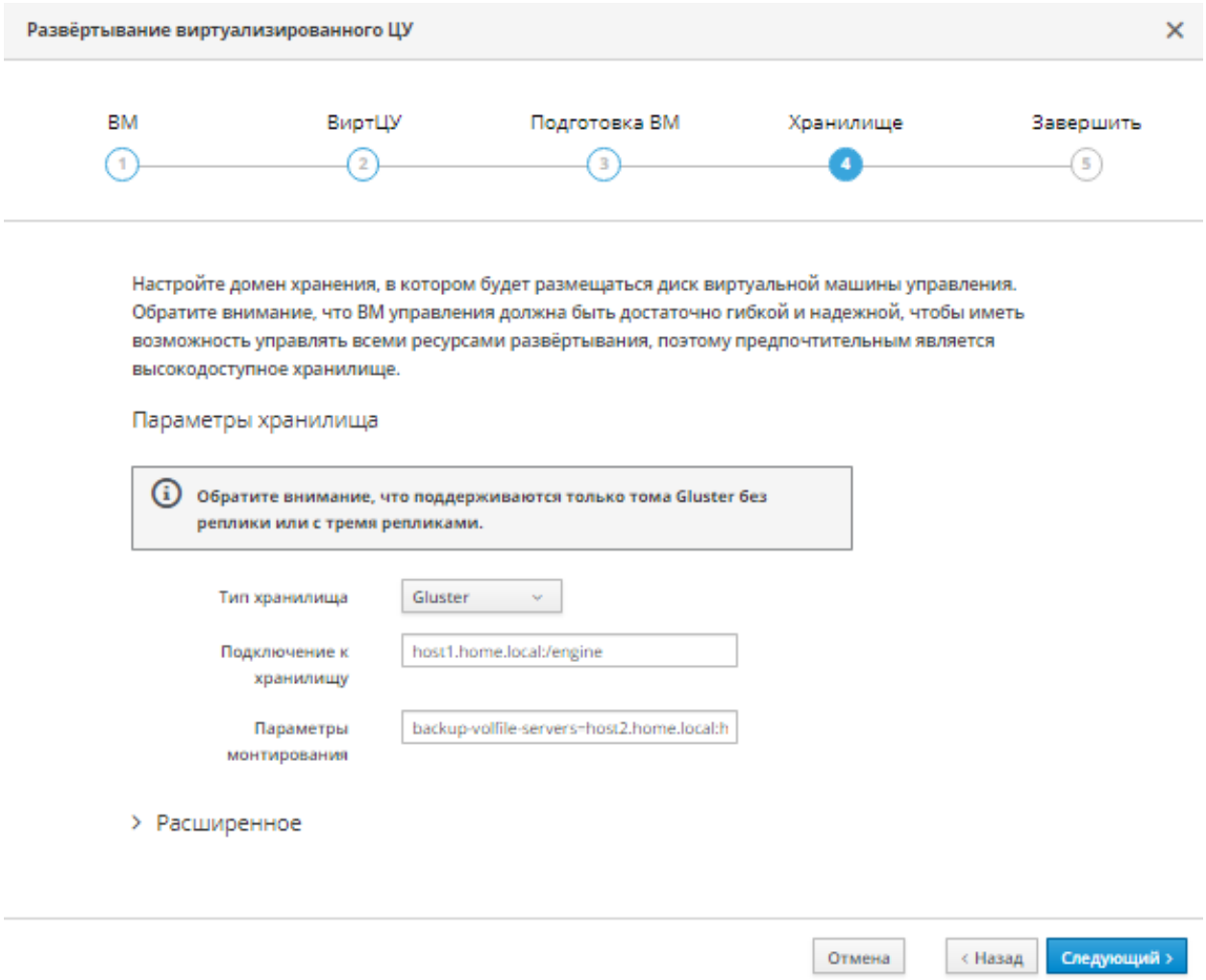

Рисунок 48 – Параметры хранилища типа Gluster

3.5.2.4.1 Настройка хранилища типа Gluster

При выборе типа хранилища Gluster, созданного в п. 3.5.1, нужно указать 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 нужно указать в поле "Подключение к хранилищу" путь к хранилищу (например, rvhost1.rosa.lan:/data/engine), созданному в п. 3.4.1 (рисунок 49).

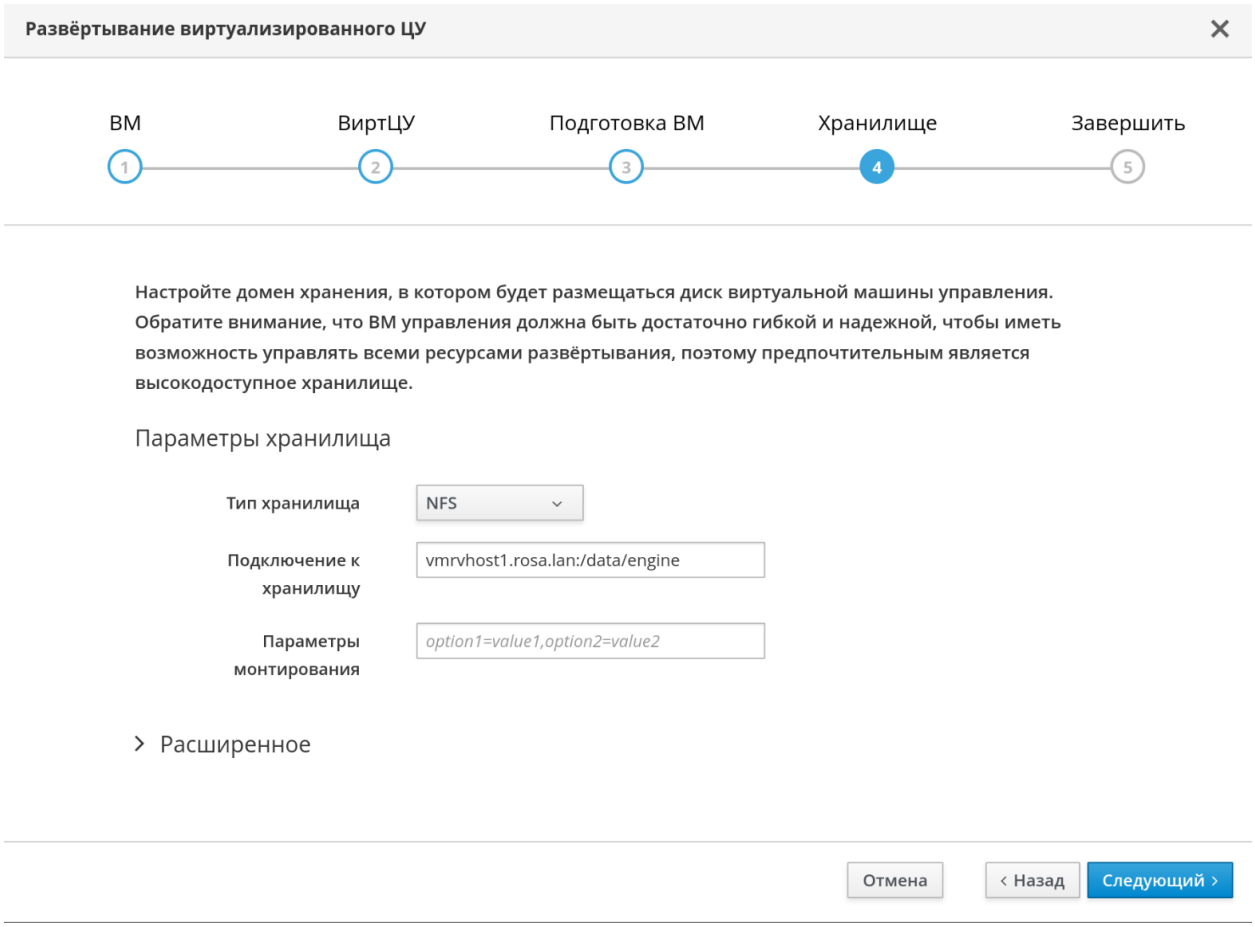

Рисунок 49 – Параметры хранилища типа NFS

3.5.2.4.3 Настройка расширенных параметров

Для настройки расширенных параметров можно нажать на "Расширенное" (рисунок 50) и заполнить поля:

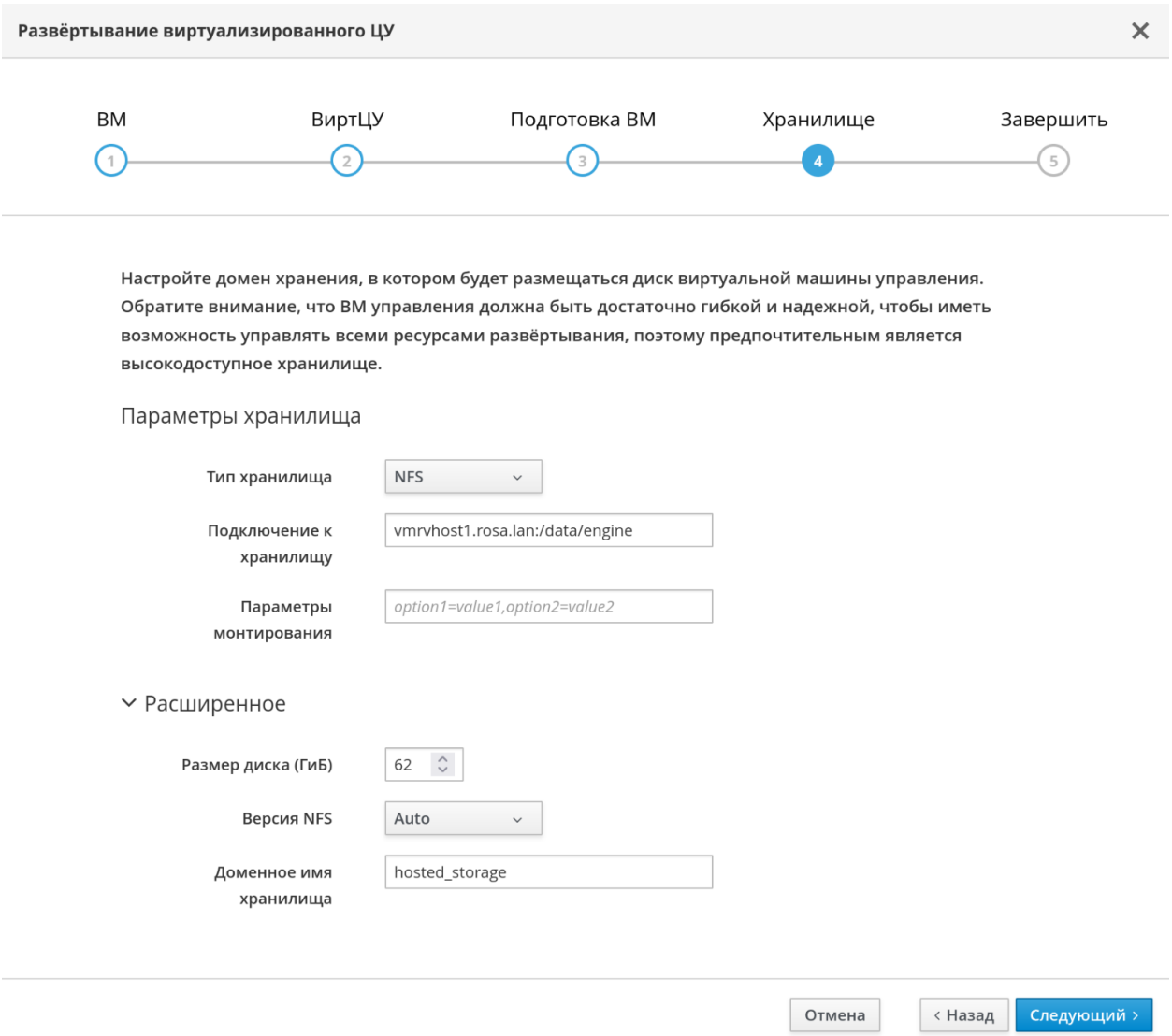

Рисунок 50 – Настройка расширенных параметров для хранилища типа NFS

– 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

Для настройки параметров хранилища типа iSCSI (рисунок 51) нужно заполнить поля:

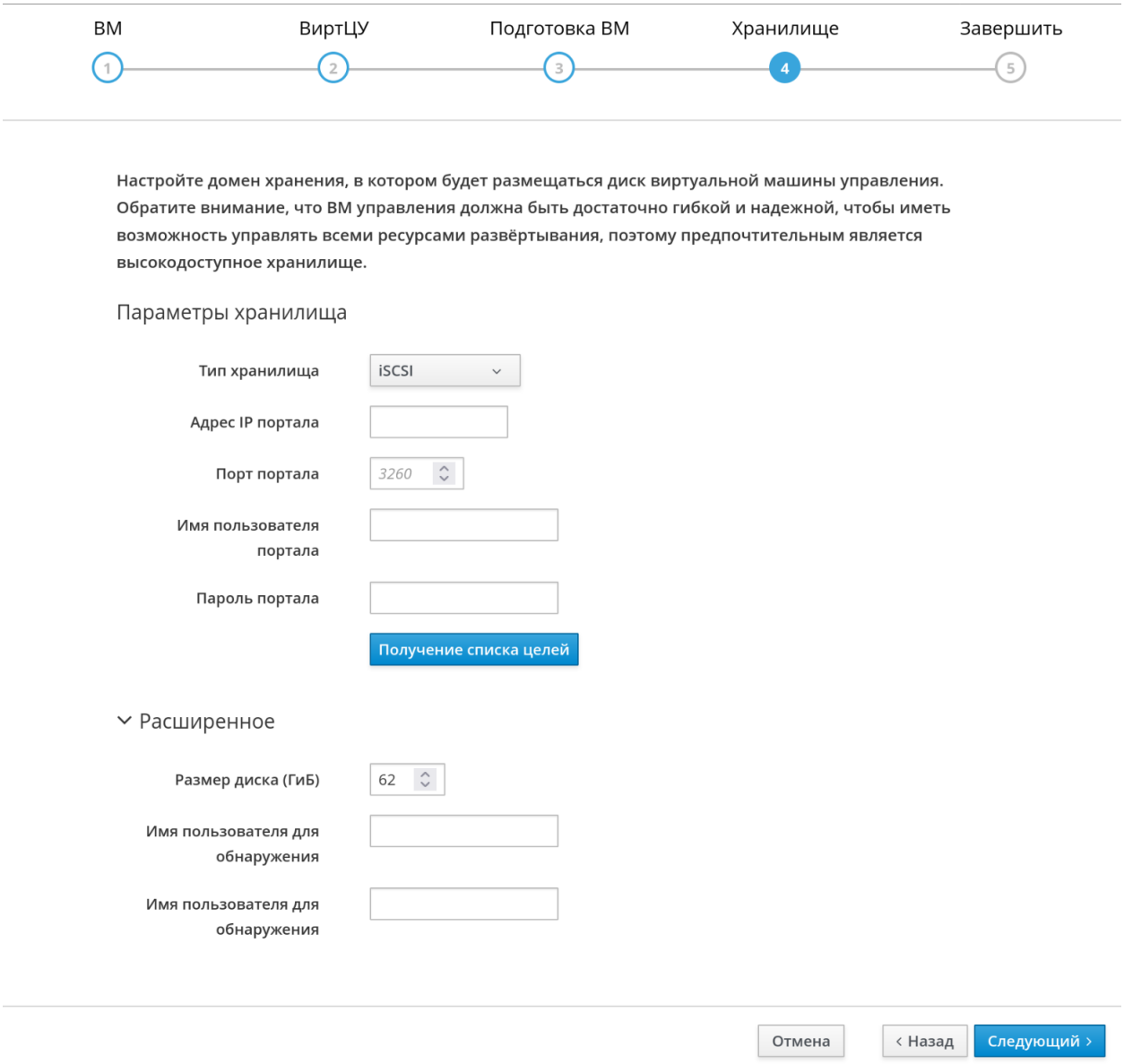

Рисунок 51 – Параметры хранилища типа iSCSI

– 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 следует нажать кнопку Получение списка целей для настройки параметров хранилища.

Затем нужно нажать 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 РОСА Виртуализация. Предварительно должна быть развернута базовая конфигурация РОСА Виртуализация, предназначенная для использования в промышленном режиме функционирования с использованием хранилища типа NFS, Gluster или iSCSI.

Процедура подключения хранилища CephFS подробно описана в п. 3.8 документа "РОСА Виртуализация 4. Руководство администратора. Часть 3. Эксплуатация".

3.5.2.4.5.1 Требования к программным и аппаратным средствам для подключения хранилища CephFS

Средство виртуализации РОСА Виртуализация:

– Развернута базовая конфигурация РОСА Виртуализация, предназначенная для использования в промышленном режиме функционирования в качестве средства виртуализации вычислительных центров.

– Используется версия РОСА Виртуализация 4.0 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" нужно нажать кнопку Завершить развертывание для переноса ВМ СУСВ в хранилище и завершения процедуры установки СУСВ (рисунок 52).

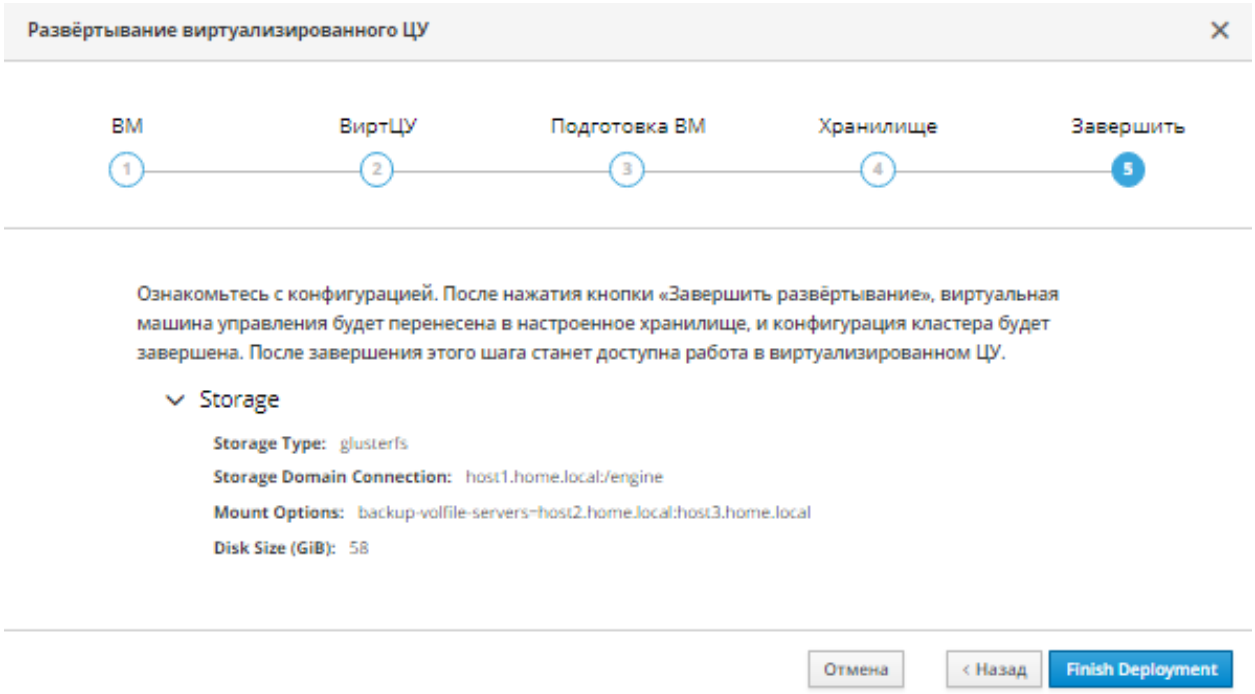

Рисунок 52 – Обзор конфигурации хранилища

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

Затем следует нажать кнопку Закрыть для завершения работы программы установки СУСВ.

3.5.3 Очистка параметров установки СУСВ

В случае неудачного завершения установки СУСВ требуется осуществить процедуру очистки данных перед повторной установкой. Для этого в консоли хоста нужно **дважды** выполнить 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 нужно выполнить в консоли хоста следующую команду:

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

Далее требуется следовать 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 нужно:

а) перейти по адресу URL Портала администрирования и на странице приветствия нажать на ссылку "CA сертификат центра управления" (рисунок 54).

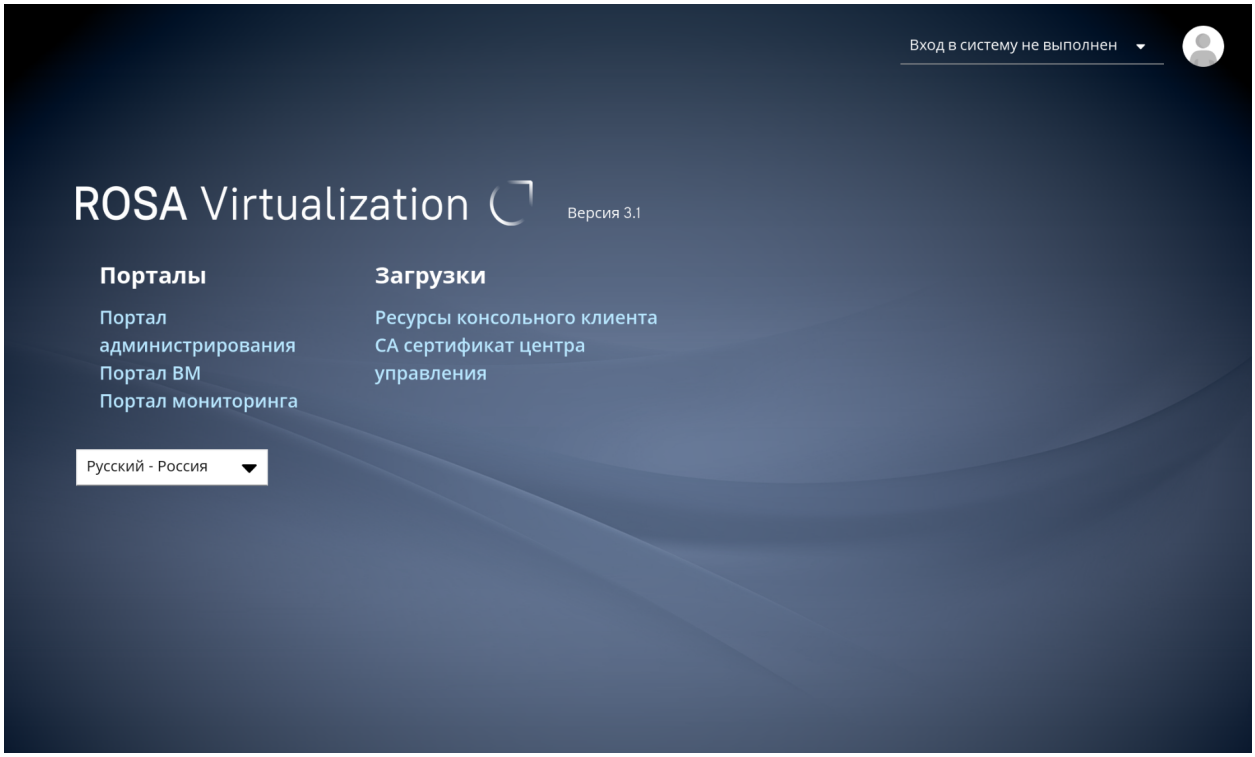

Рисунок 54 – Портал входа РОСА Виртуализация: Портал администрирования, Портал ВМ

б) после того, как будет загружен файл pki-resource (без расширения), открыть окно "Параметры/Предпочтения":

– Windows – открыть меню Firefox и выбрать "Настройки" (URL about:preferences);

– Mac – открыть меню Firefox и выбрать "Параметры...";

– Linux – открыть меню "Правка" и выбрать "Параметры";

в) выбрать в меня слева раздел "Приватность и защита" и прокрутить вниз содержимое формы до секции "Сертификаты" (рисунок 55);

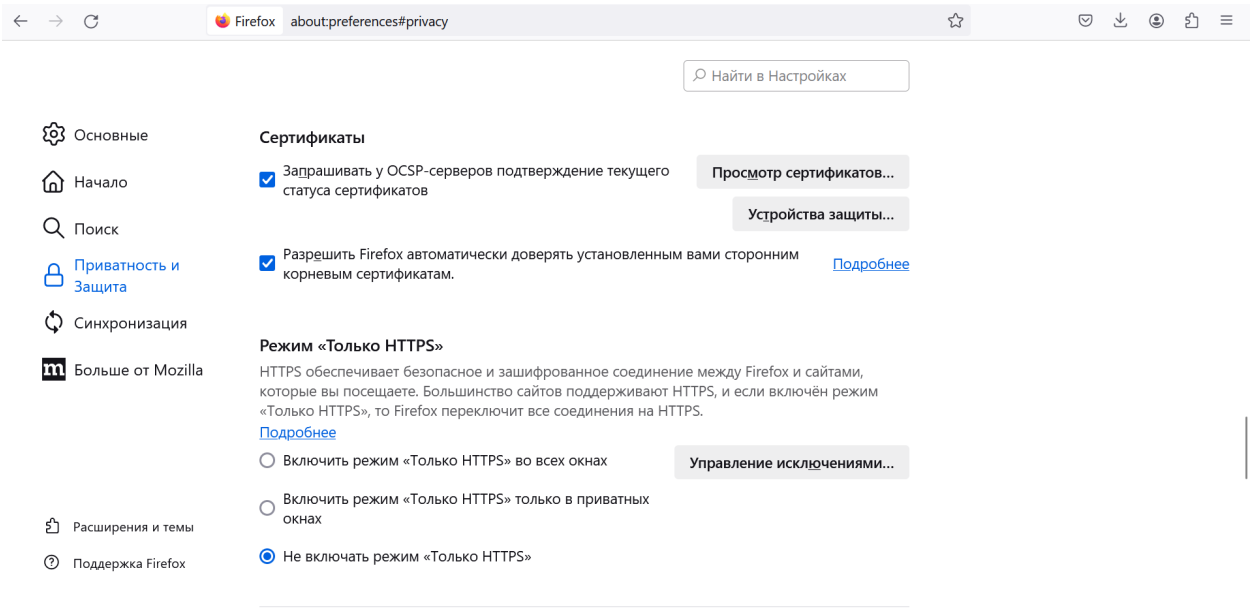

Рисунок 55 – Firefox: Раздел "Приватность и защита", секция "Сертификаты"

г) нажать Просмотр сертификатов..., чтобы открыть "Управление сертификатами" и перейти на вкладку "Центры сертификации" (рисунок 56);

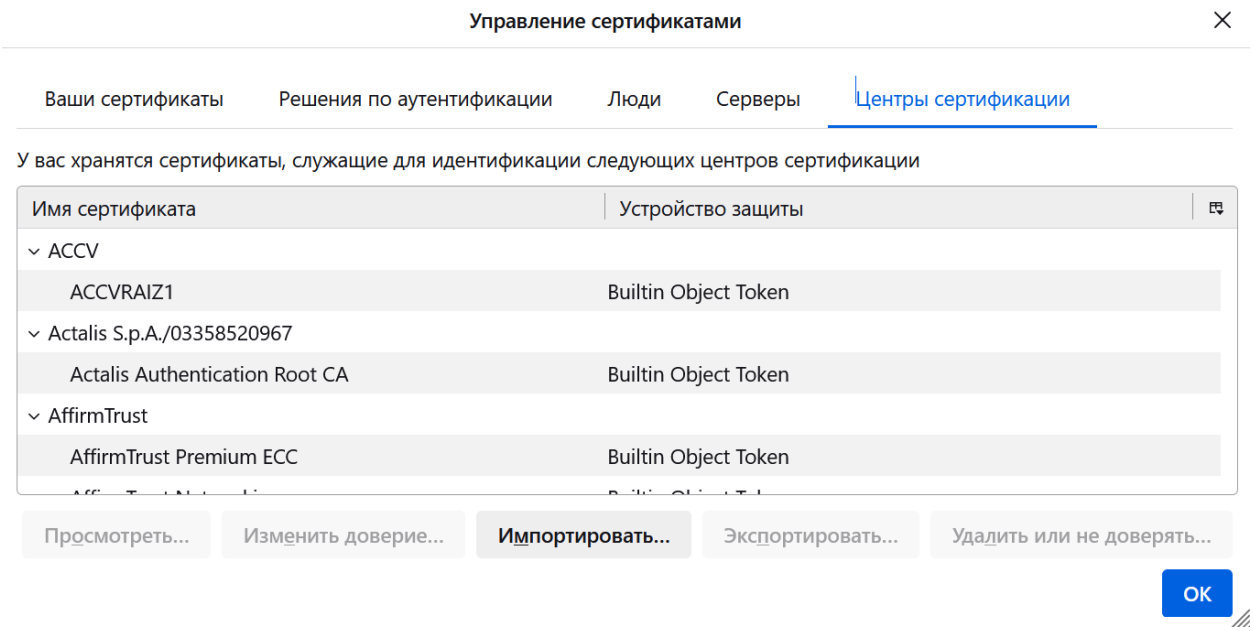

Рисунок 56 – Firefox: "Управление сертификатами" – вкладка "Центры сертификации"

д) нажать на кнопку Импортировать... (рисунок 56);

е) выбрать файл корневого сертификата, который нужно импортировать (для просмотра загруженного файла сменить тип файла на "Все файлы");

ж) отметить флажками параметры доверия и нажать кнопку `OK`;

з) в разделе Диспетчера сертификатов нажать кнопку `OK` и закрыть окно "Параметры/Предпочтения";

и) убедиться в том, что все процессы Firefox остановлены;

к) перезапустить Firefox и перейти по адресу URL Портала администрирования.

Значок 🔒 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 требуется:

а) перейти по адресу URL Портала ВМ и на странице приветствия нажать на кнопку `CA сертификат центра управления` (рисунок 57);

б) после того, как будет загружен файл pki-resource.cer (расширение файла .cer) перейти в меню "Настройки → Конфиденциальность и безопасность → Настроить сертификаты" (рисунок 57) и нажать на значок ↗ для вызова диалога управления сертификатами (URL chrome://settings/security);

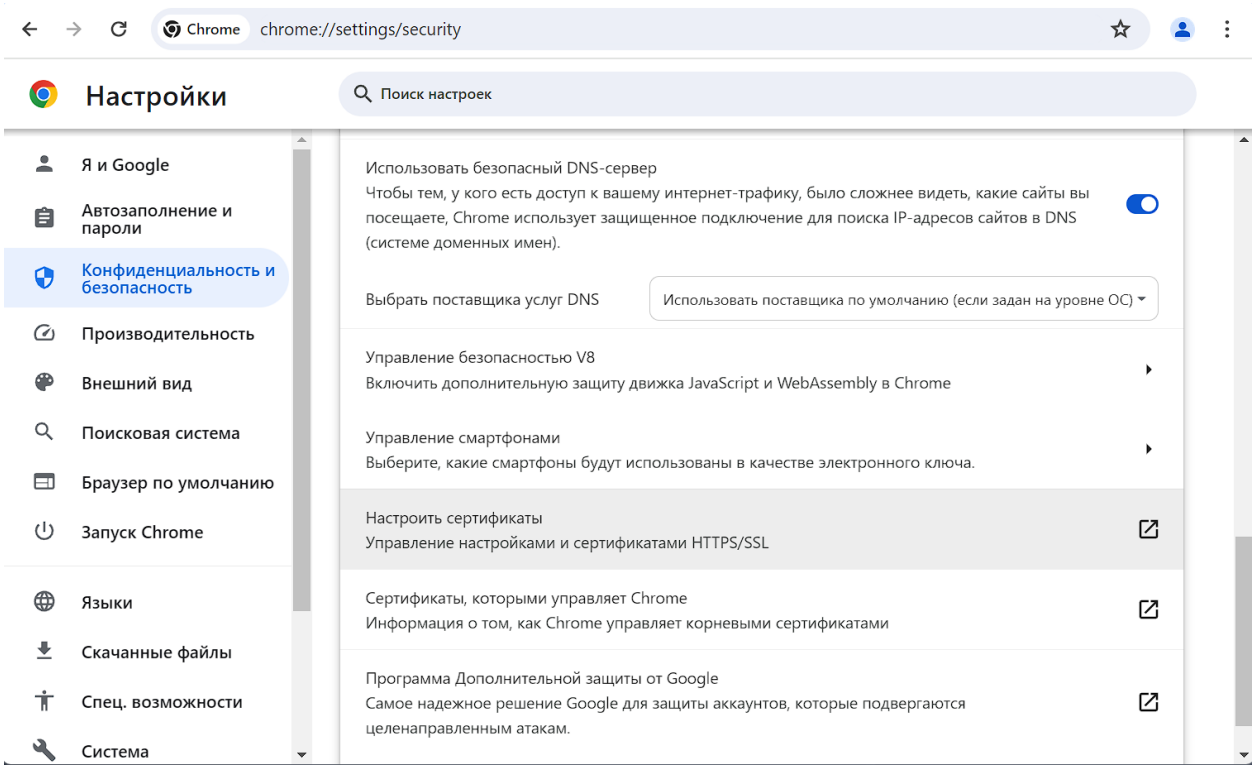

Рисунок 57 – Chrome: Настройки → Конфиденциальность и безопасность → Настроить сертификаты

в) в диалоге управления сертификатами нажать кнопку `Импорт…` (рисунок 58);

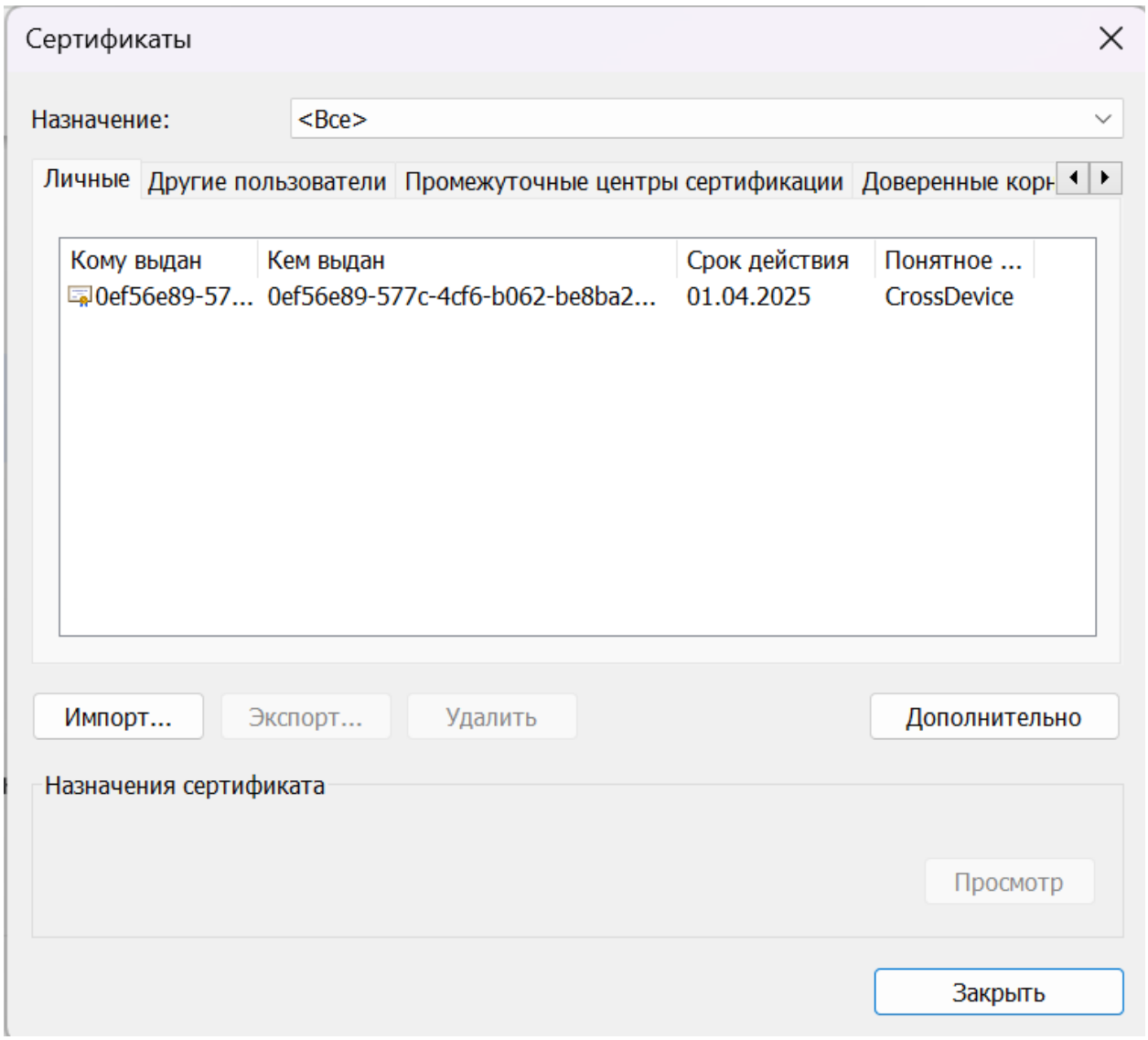

Рисунок 58 – Chrome: диалог для управления сертификатами

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

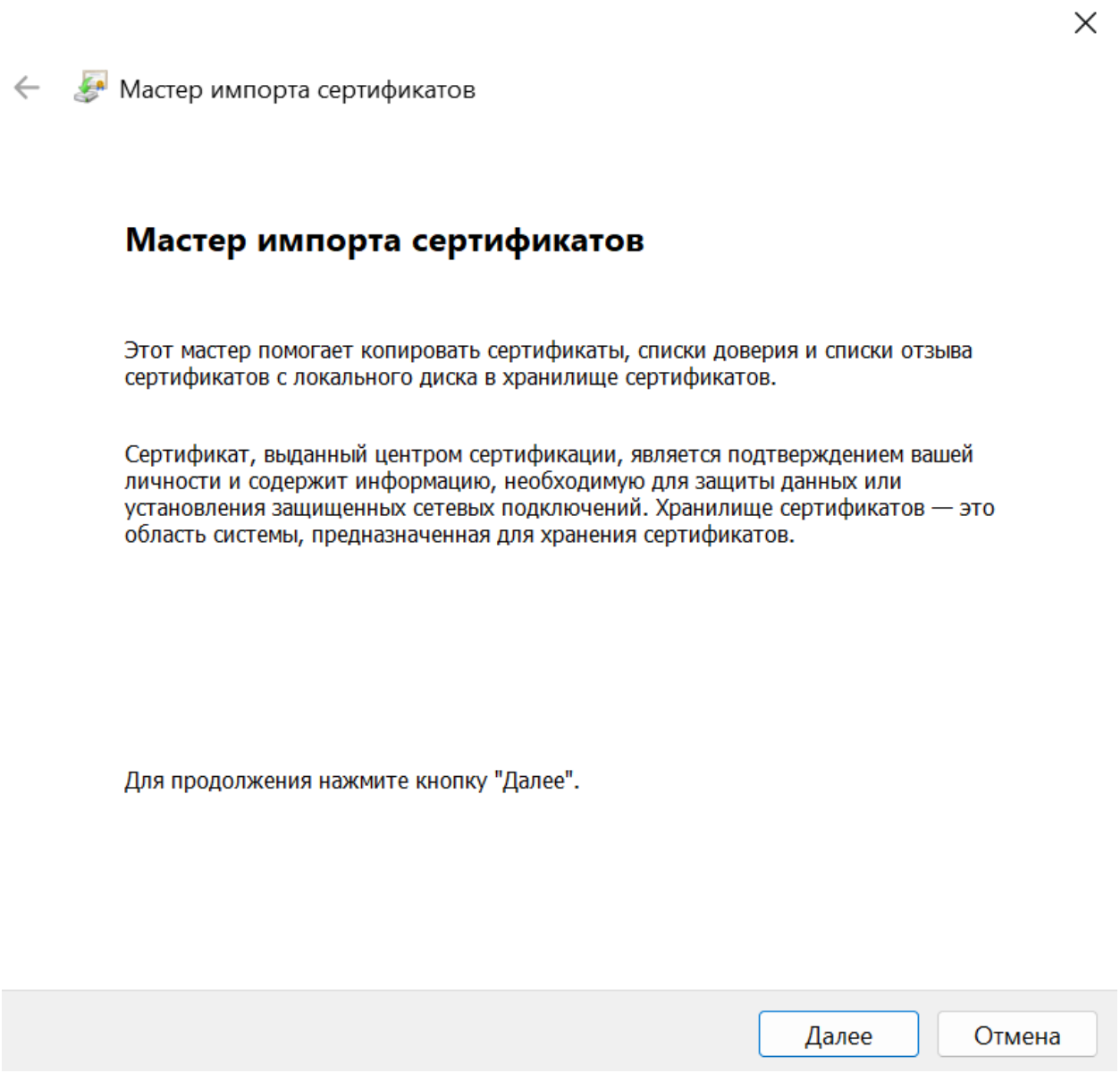

Рисунок 59 – Мастер импорта сертификатов (Windows)

г) нажать кнопку Далее;

д) в "Мастере импорта сертификатов" указать "Импортируемый файл", для чего нажать на кнопку Обзор… (рисунок 60);

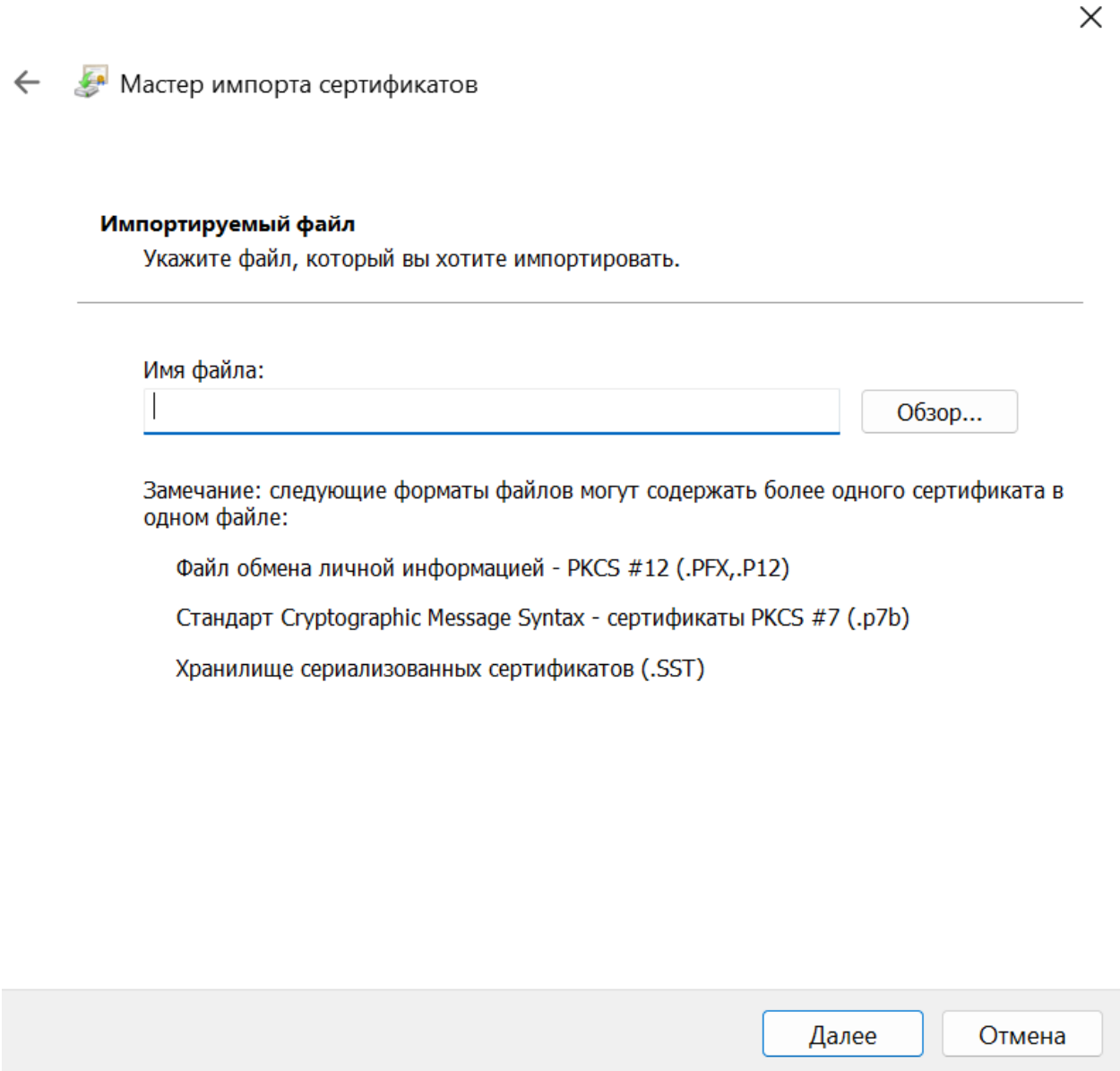

Рисунок 60 – Мастер импорта сертификатов – выбор Импортируемый файл

е) выбрать файл корневого сертификата X.509, который нужно импортировать (рисунок 61), для чего сменить тип просмотра файлов на "Все файлы" и открыть ранее загруженный файл pki-resource.cer;

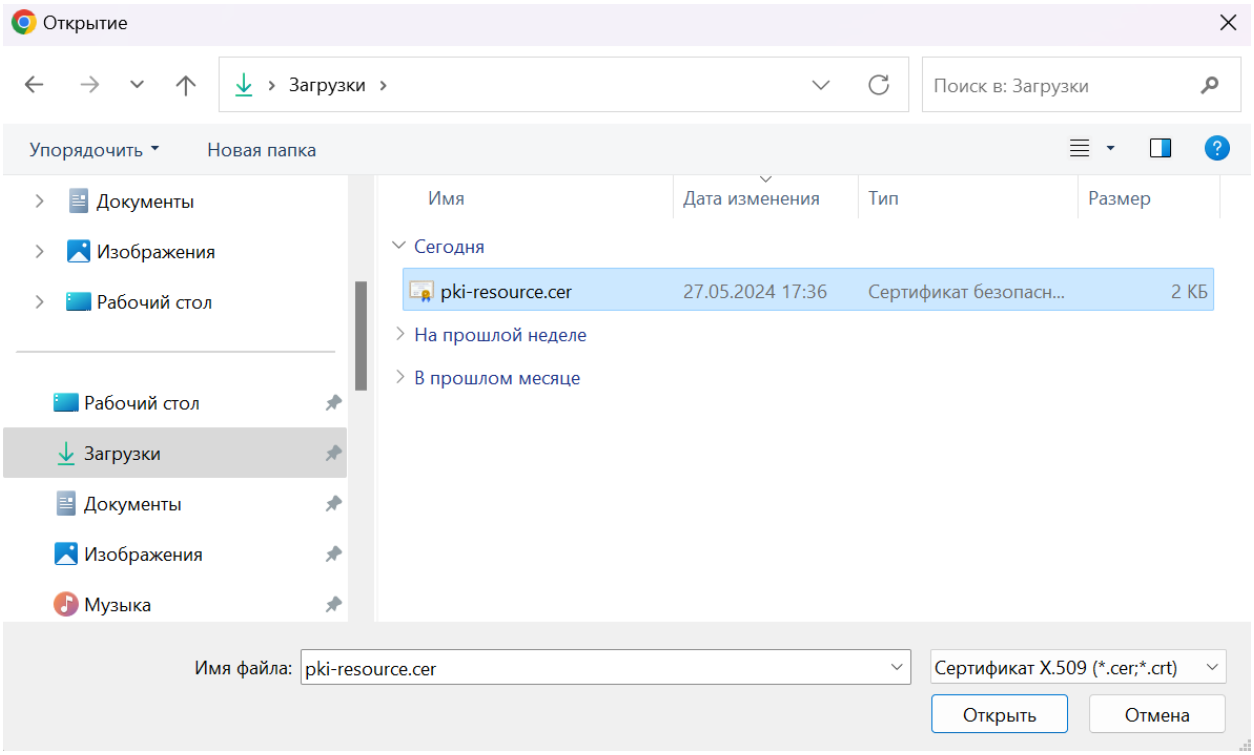

Рисунок 61 – Выбор файла корневого сертификата X.509 (Windows)

ж) в "Мастере импорта сертификатов" указать необходимое "Хранилище сертификатов" из "Доверенных корневых центров сертификации" (рисунок 62) и нажать на кнопку Далее;

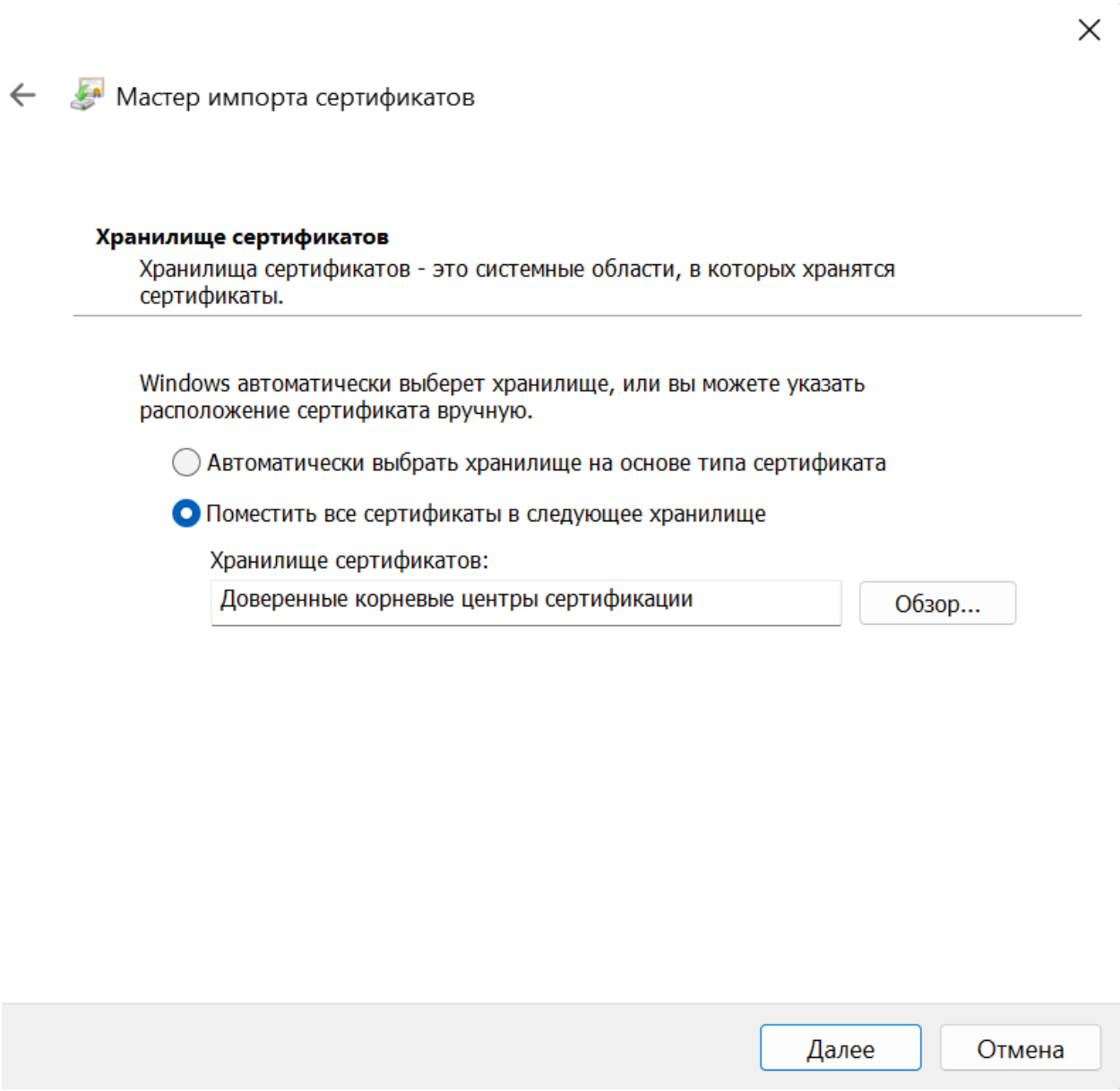

Рисунок 62 – Мастер импорта сертификатов: Хранилище сертификатов – Доверенные корневые центры сертификации

з) в завершающем диалоге "Мастера импорта сертификатов" нажать на кнопку Готово (рисунок 63).

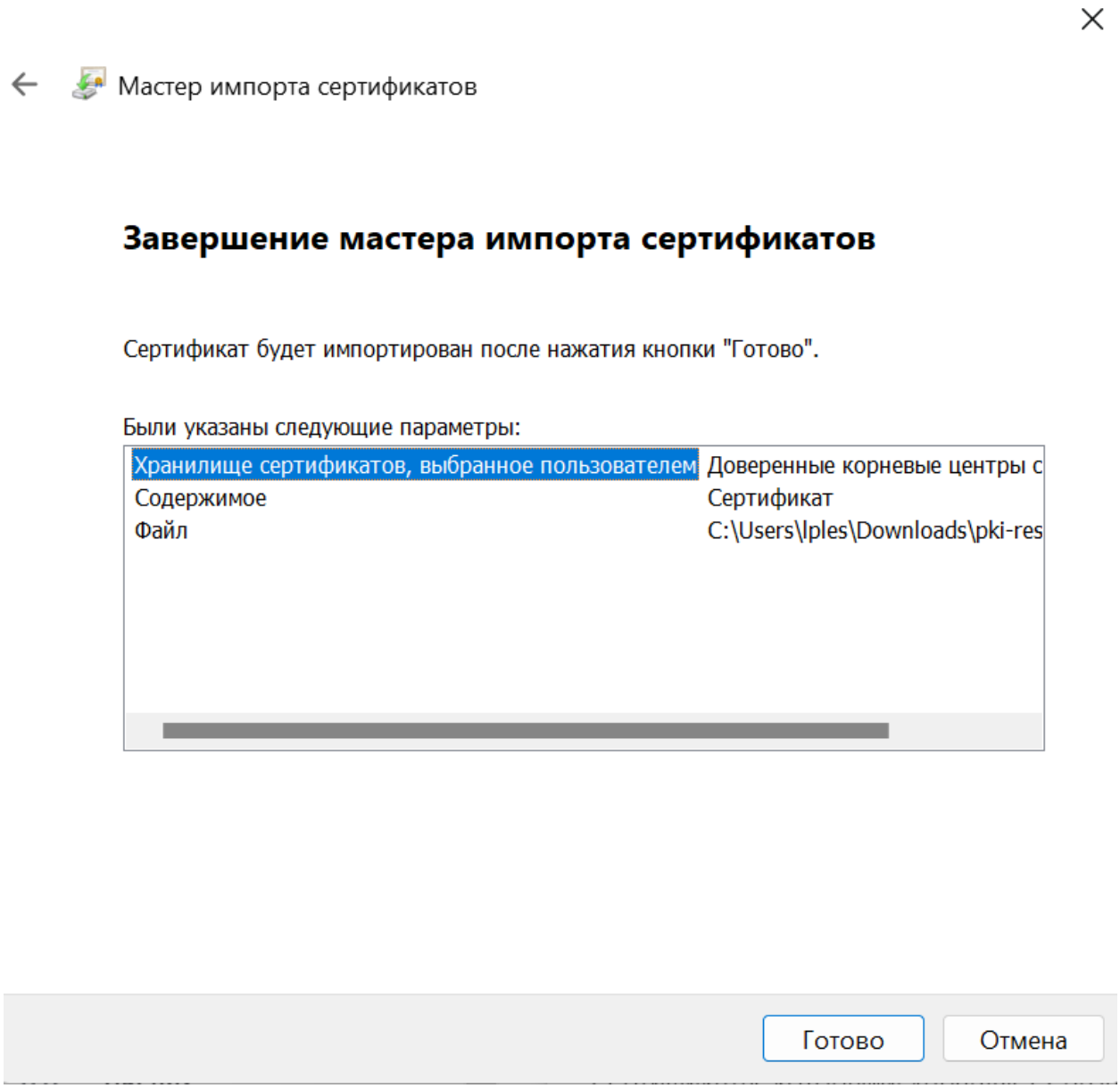

Рисунок 63 – Завершающий диалог "Мастера импорта сертификатов"

и) закрыть Chrome и убедиться в том, что все процессы Chrome остановлены;

к) перезапустить Chrome и перейти по адресу URL Портала администрирования (СУСВ). Значок в адресной строке указывает на то, что сертификат ЦС установлен (рисунок 64).

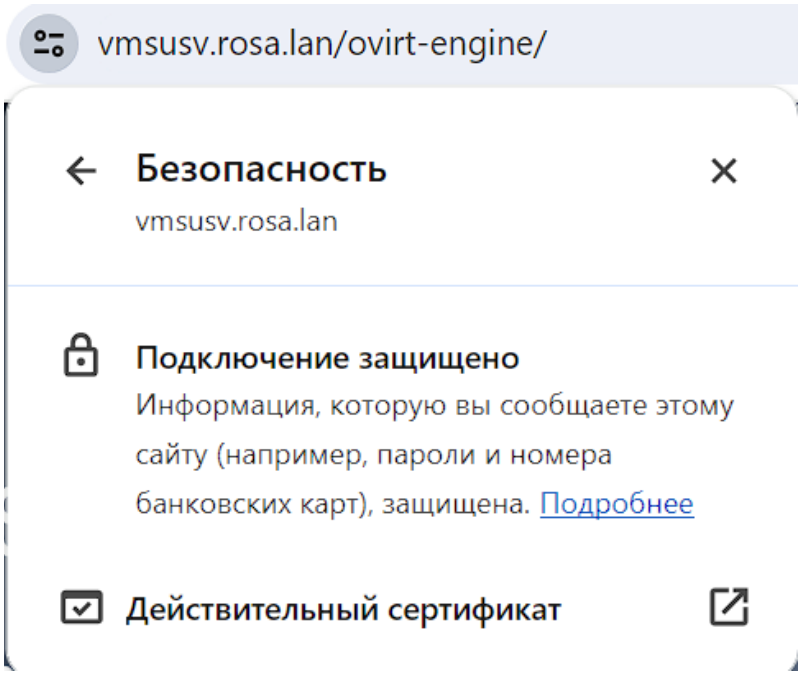

Рисунок 64 – Подключение к СУСВ (Портал администрирования) защищено

3.5.6 Вход в веб-интерфейс СУСВ

Для доступа к веб-интерфейсу необходимо ввести 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).

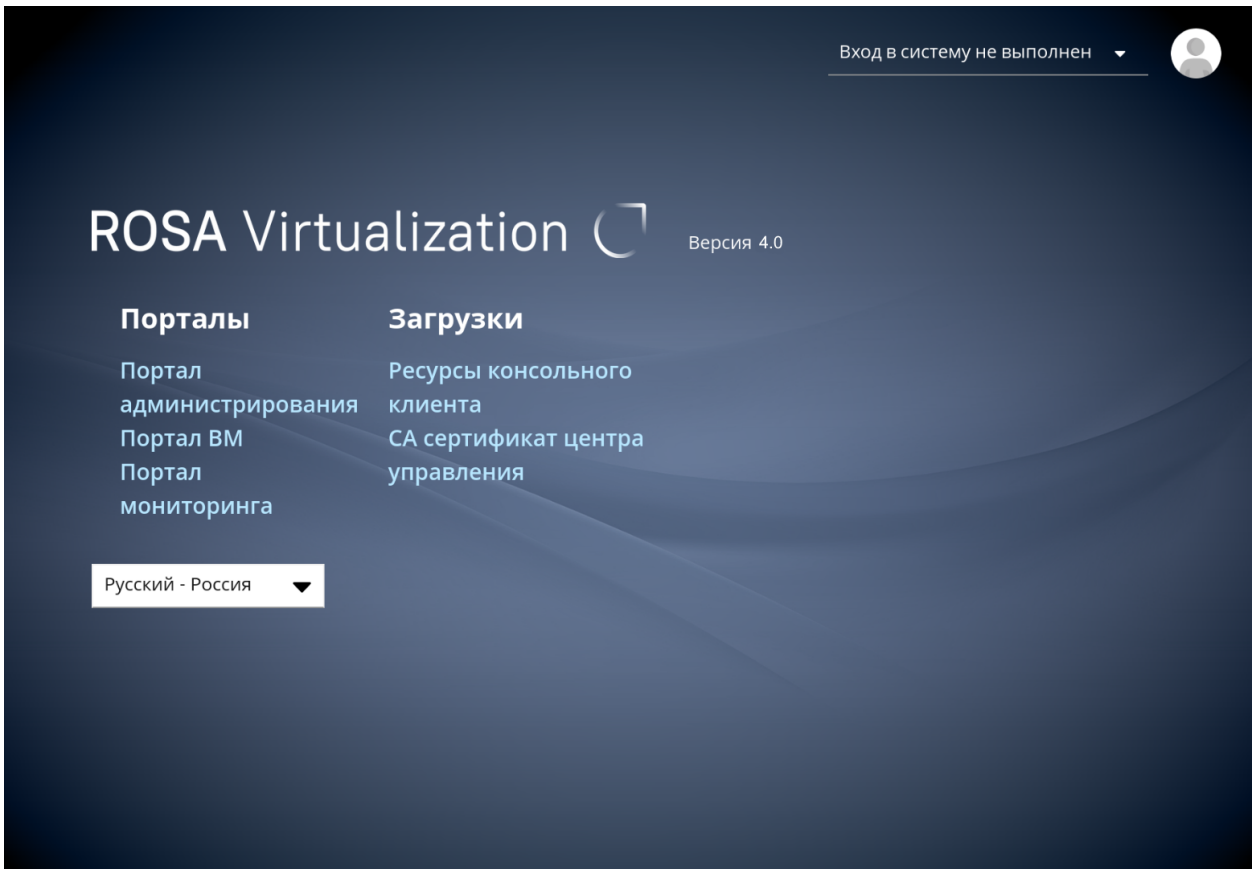

Рисунок 65 – Интерфейс выбора портала: Портал администрирования, Портал ВМ

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

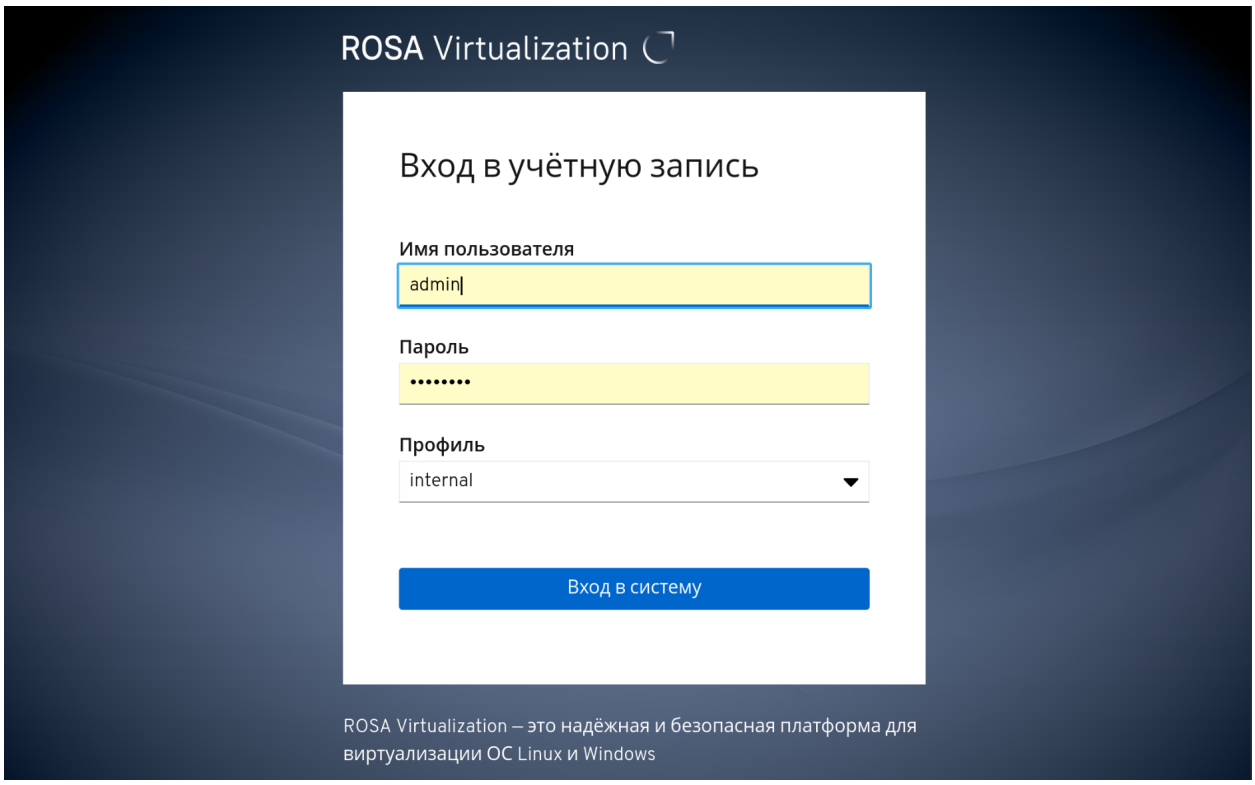

Рисунок 66 – Вход в учётную запись РОСА Виртуализация

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

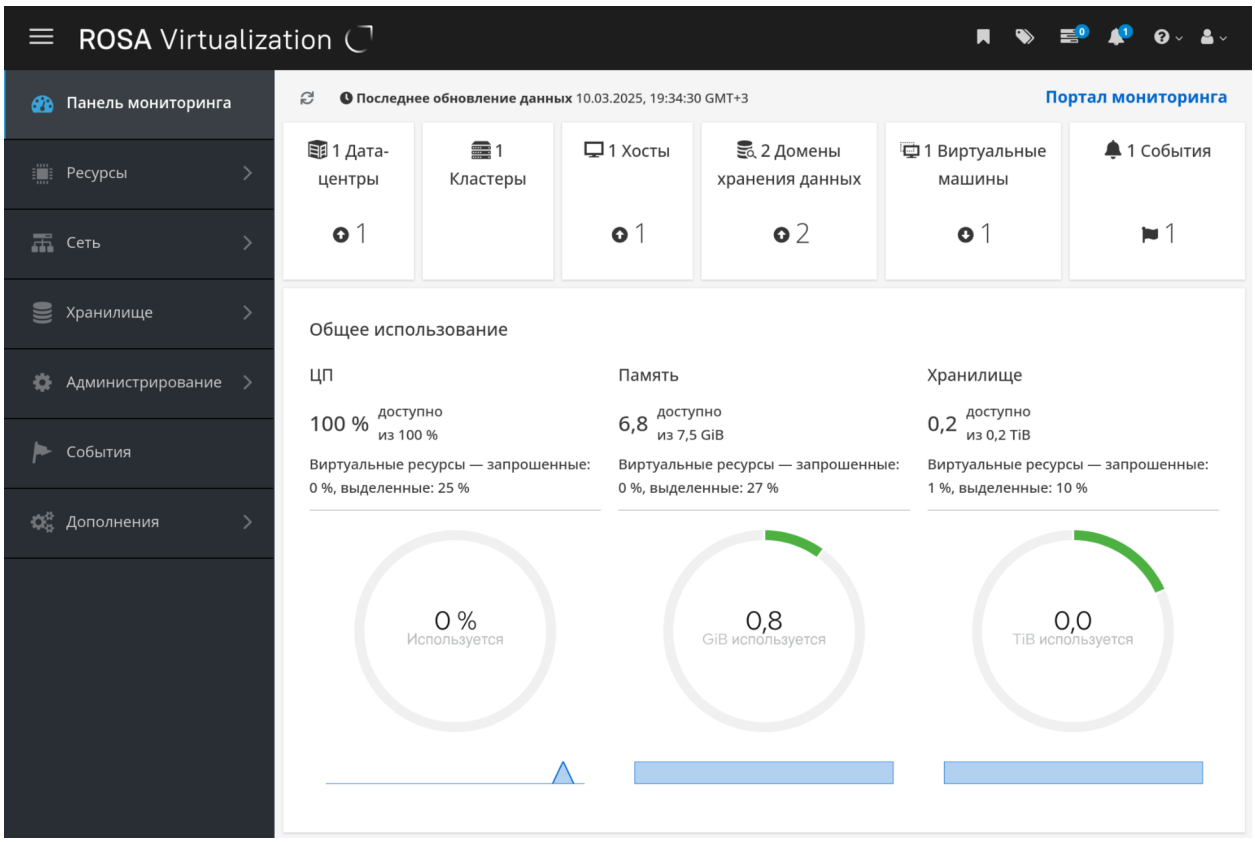

Рисунок 67 – Панель мониторинга СУСВ

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

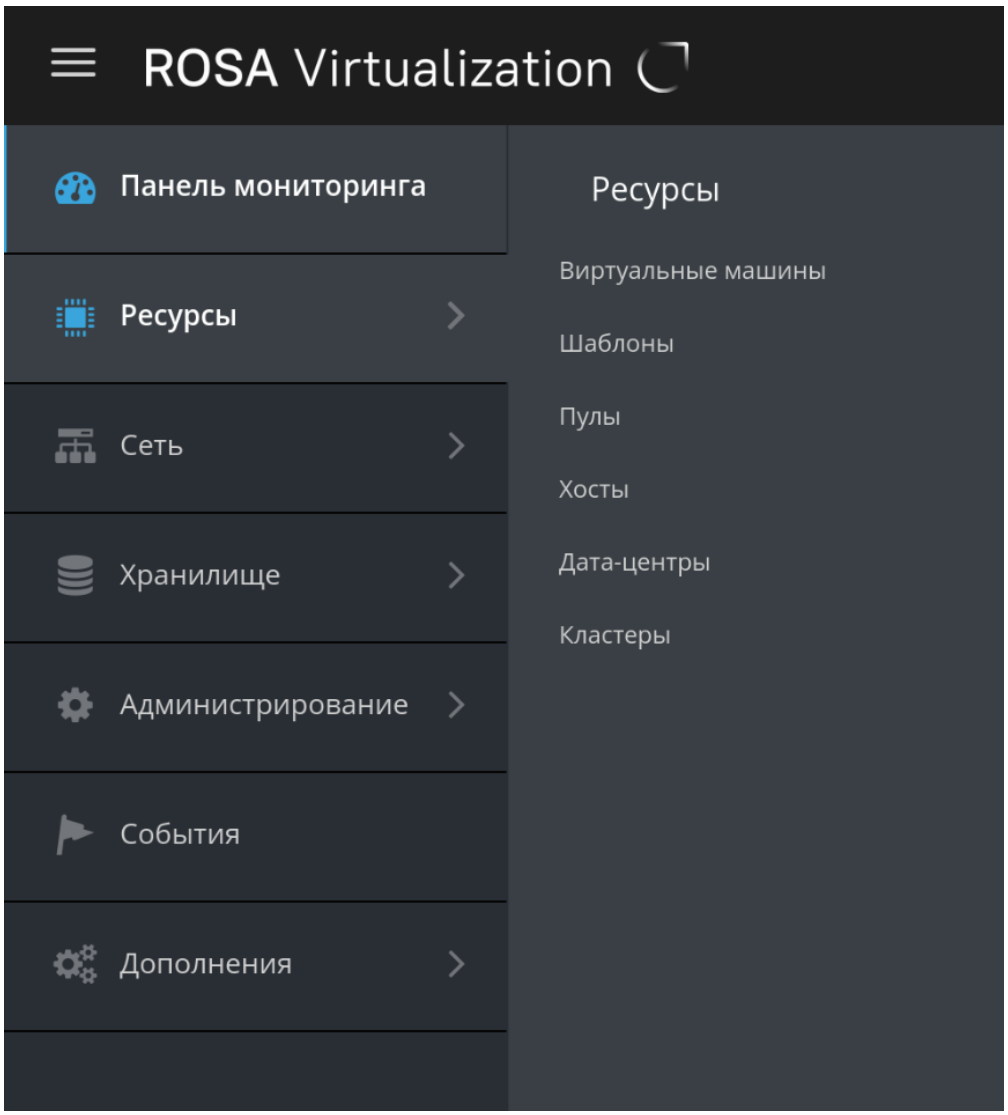

Рисунок 68 – Главное меню веб-интерфейса СУСВ с открытым подменю "Ресурсы"

3.6 Добавление хостов в кластер

При развертывании РОСА Виртуализация в базовой конфигурации требуется выполнить 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 РОСА Виртуализация должен принадлежать определенному кластеру.

Во время установки РОСА Виртуализация 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 нужно:

а) выбрать пункт "Ресурсы → Хосты" в главном меню СУСВ и нажать кнопку Добавить. На экране появится вкладка "Общее" окна "Новый хост" (рисунок 69).

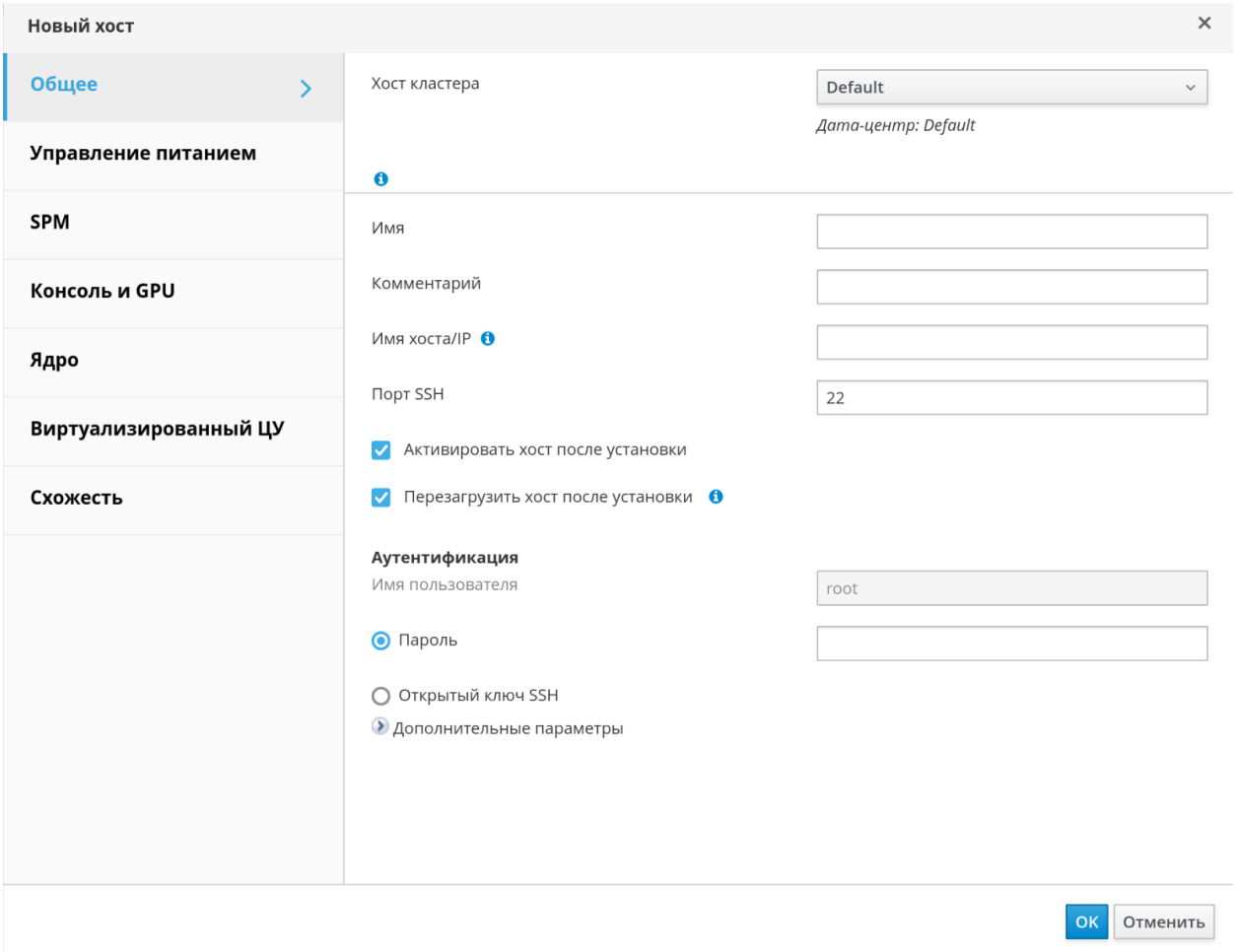

Рисунок 69 – Вкладка "Общее" окна "Новый хост"

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

в) в поле "Пароль" указать пароль учетной записи суперпользователя root данного хоста;

г) перейти на вкладку "Виртуализированный ЦУ" и выбрать 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 РОСА Виртуализация;

д) для применения всех сделанных изменений нажать кнопку OK;

е) для настройки политики энергосбережения на экране появится окно "Параметры управления питанием". При необходимости в настройке параметров агента интерфейса низкоуровнего управления питанием хоста нажать кнопку Настроить управление питанием и ввести необходимые параметры;

ж) для завершения процедуры добавления хоста в кластер нажать кнопку ОК.

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

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

3.7 Активация лицензии РОСА Виртуализация

Лицензия РОСА Виртуализация 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 РОСА Виртуализация 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

Графический интерфейс системы лицензирования являются частью интерфейса РОСА Виртуализация и устанавливается из отдельного дистрибутива.

Для активации лицензии РОСА Виртуализация требуется открыть меню "Дополнения" Портала администрирования и выбрать секцию "Лицензирование".

В открывшемся окне для управления лицензированием РОСА Виртуализация нажать на кнопку Установить лицензию для начала процесса установки лицензии (рисунок 70).

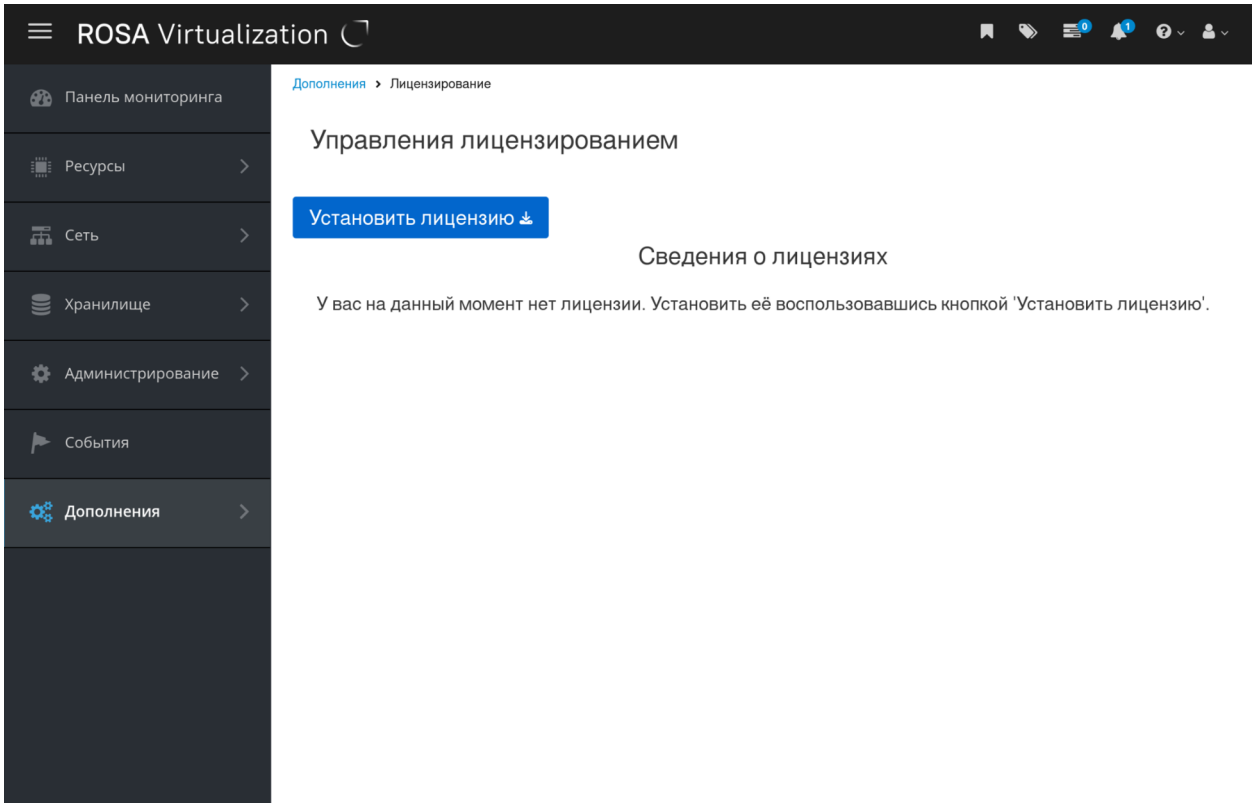

Рисунок 70 – Управление лицензированием РОСА Виртуализация

На экране откроется форма для установки лицензии (рисунок 71). В этой форме есть два варианта установки лицензий:

– Установка путем вставки скопированного ключа лицензии.
– Установка путем вставки файла лицензий.

3.7.1.1 Установка ключа лицензии

Если имеется лицензия (электронный ключ активации) в виде текстового файла, можно скопировать его содержимое в буфер обмена и вставить в поле ввода справа (поле "Вставить лицензию"). Затем нажать на кнопку Загрузить и после валидации лицензии – на кнопку Закрыть.

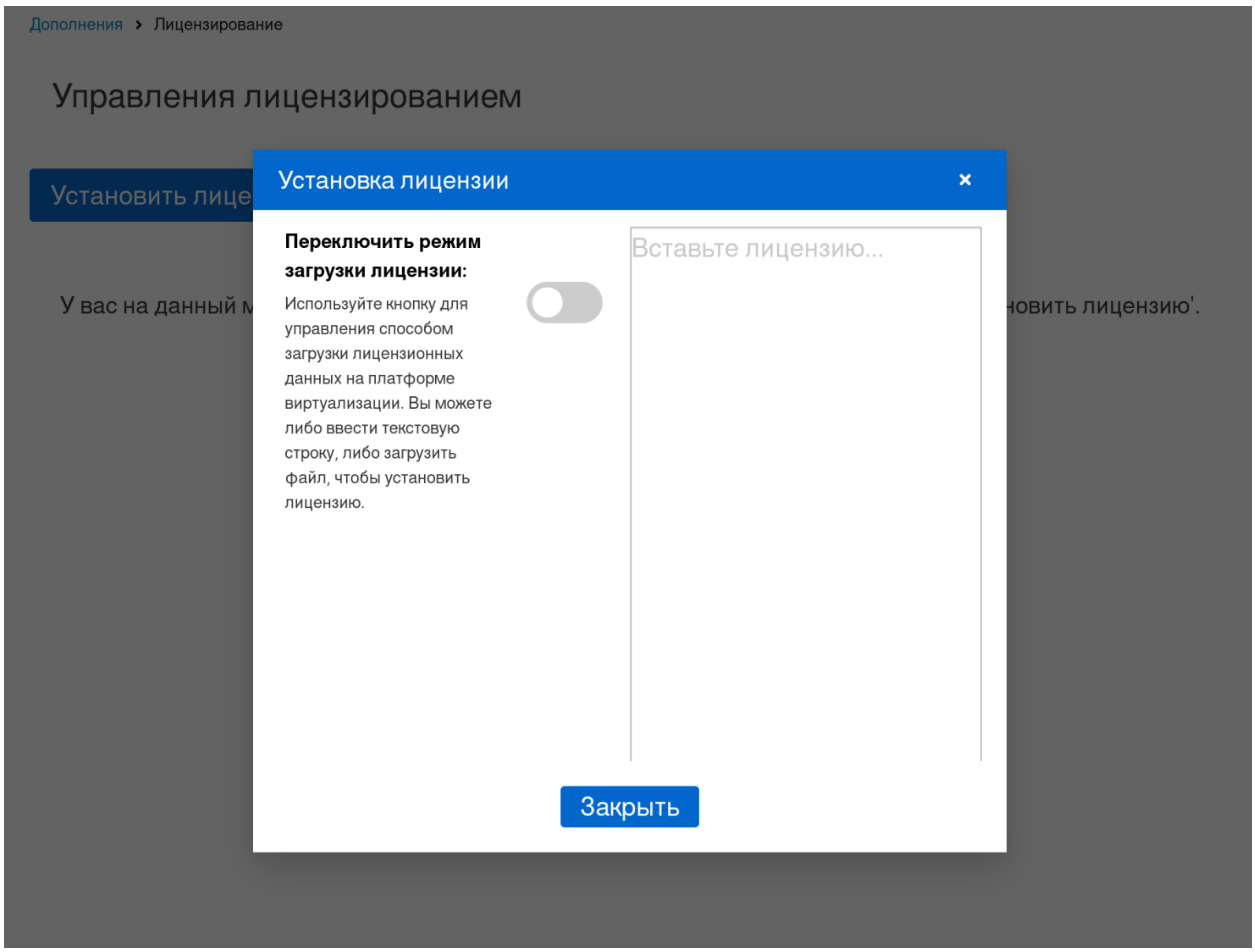

Рисунок 71 – Форма установки лицензии РОСА Виртуализация

При корректном окончании установки лицензии отобразится сообщение об успехе (рисунок 72).

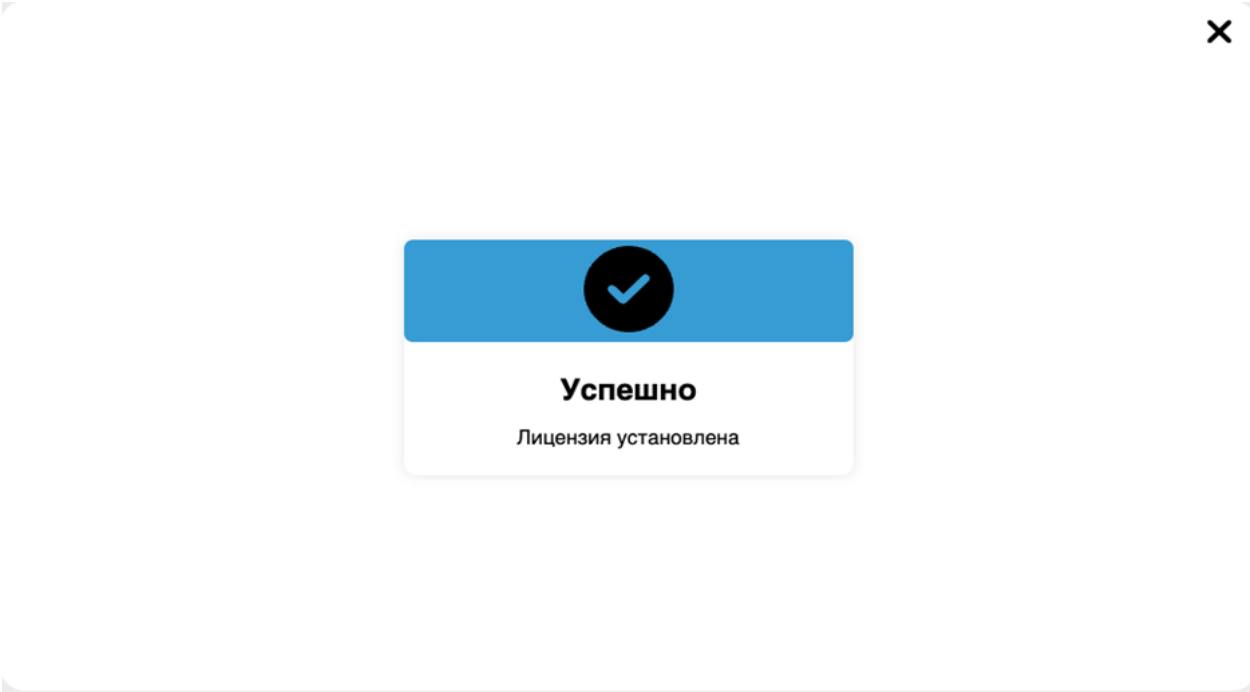

Рисунок 72 – Успешная установка лицензии

Если была допущена ошибка при установке, то отобразится сообщение об ошибке (рисунок 73).

Рисунок 73 – Ошибка установки лицензии

Действия, описанные выше, применяются при установке новой или расширяющей лицензии.

Если устанавливается лицензия с пересечением сроков действия с текущей лицензией, отобразится сообщение с предупреждением в меню установки (рисунок 1). В данном предупреждении будут описаны сроки действия лицензий. В случае согласия устанавливается новая лицензия с сообщениями об успехе или об ошибке.

3.7.1.2 Установка файла лицензии

Если требуется загрузить лицензию (электронный ключ активации) через файл, то нужно выполнить следующие действия:

а) использовать переключатель "Переключить режим загрузки лицензии" для изменения режима загрузки лицензии (рисунок 74). В данном режиме установки есть ограничение по размеру файла. Максимальный размер файла должен быть не больше 5 КБ. При включении активируется режим загрузки файла в двух вариантах:

– в окне загрузки файла нажать на кнопку `Загрузите файл`;
– переместить файл в окно загрузки файла с помощью мыши.

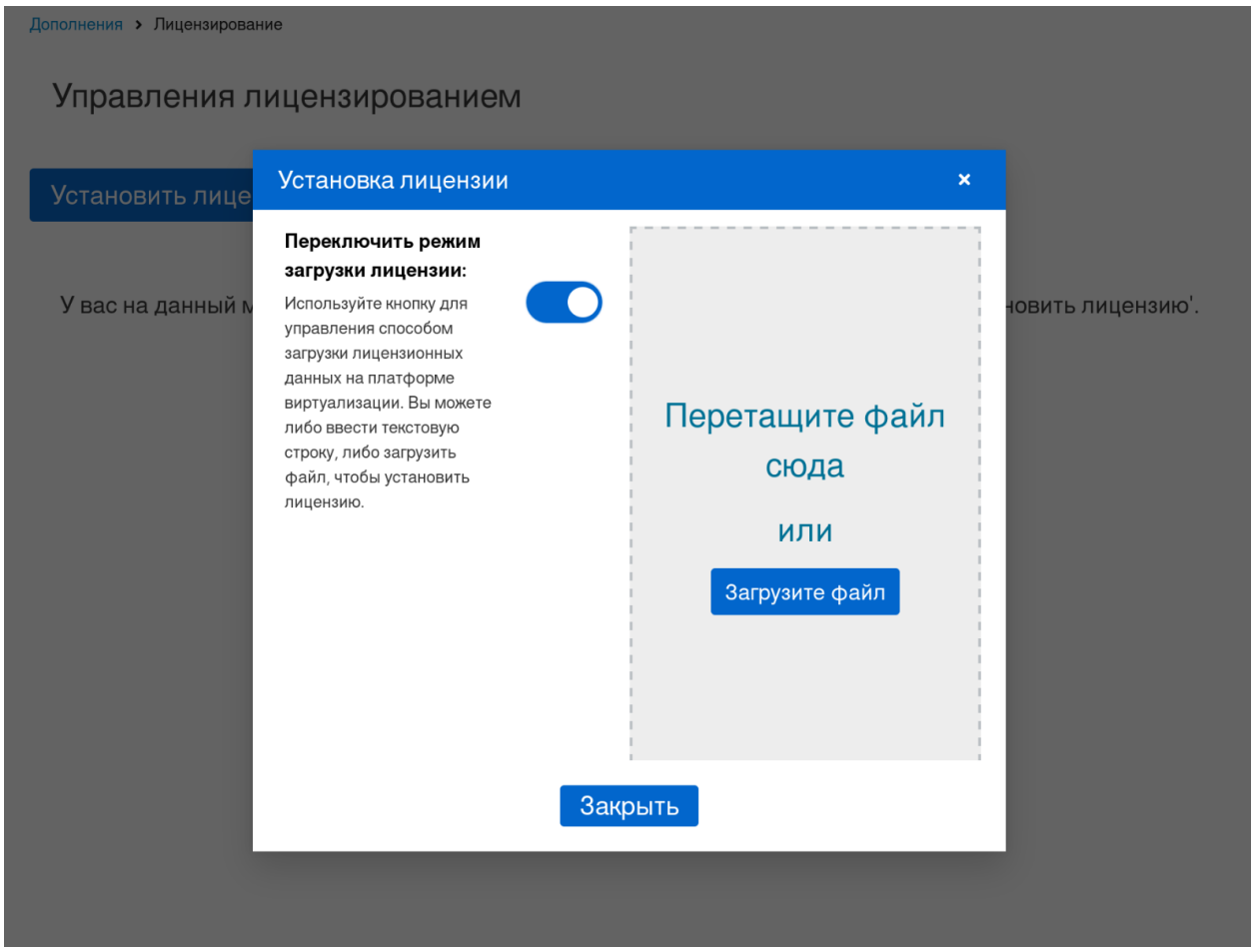

Рисунок 74 – Диалоговое окно загрузки файла лицензии

б) переместить файл с лицензией (в примере – license_rv.gz) в окно для загрузки или выбрать файл с диска, используя файловый диалог по кнопке `Загрузите файл` (рисунок 75).

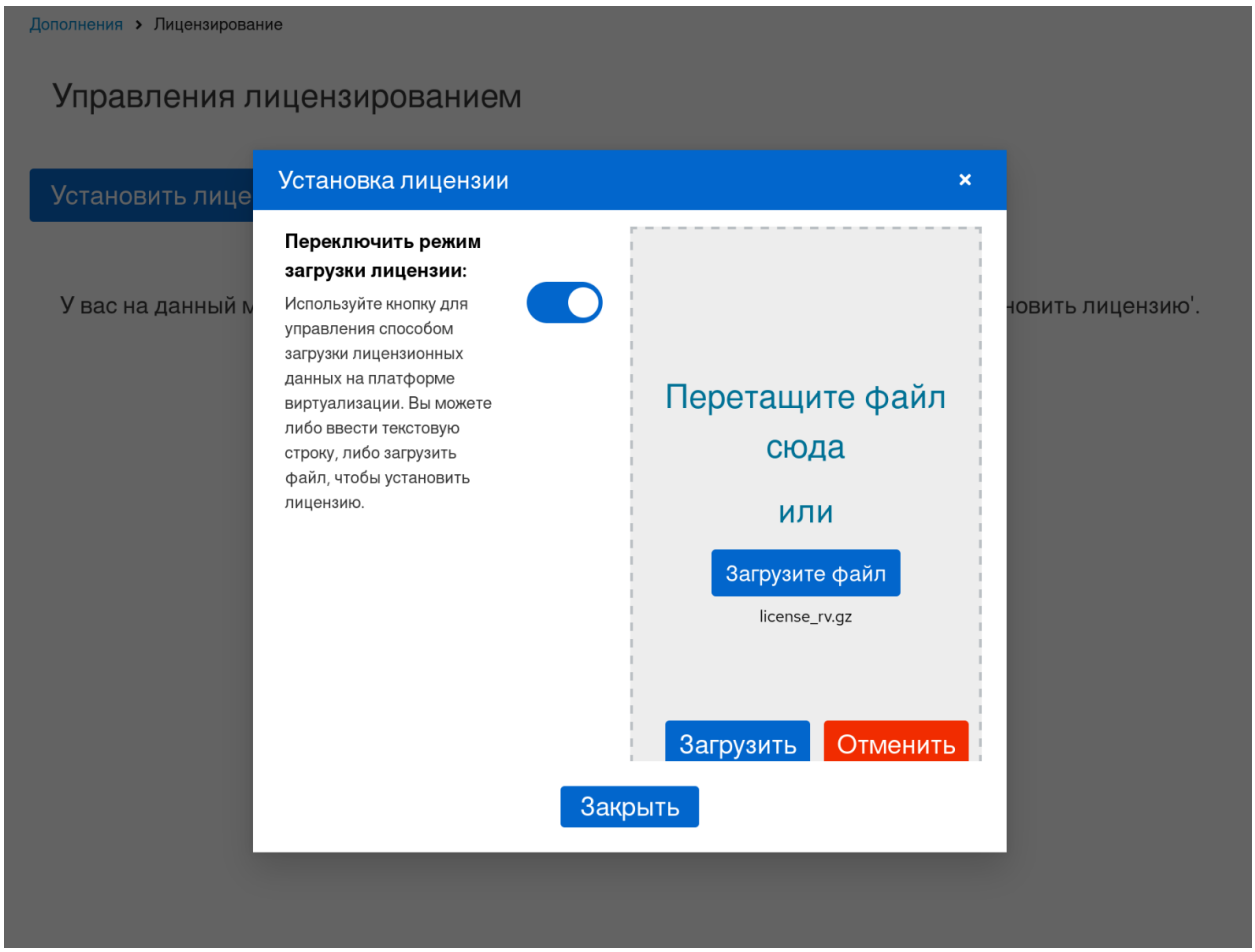

Рисунок 75 – Подтверждение загрузки лицензии

в) нажать на кнопку `Загрузить` для загрузки файла с лицензией или на кнопку `Отменить` – для отмены операции (рисунок 75).

На экране откроется окно с подтверждением загрузки лицензии (рисунок 76).

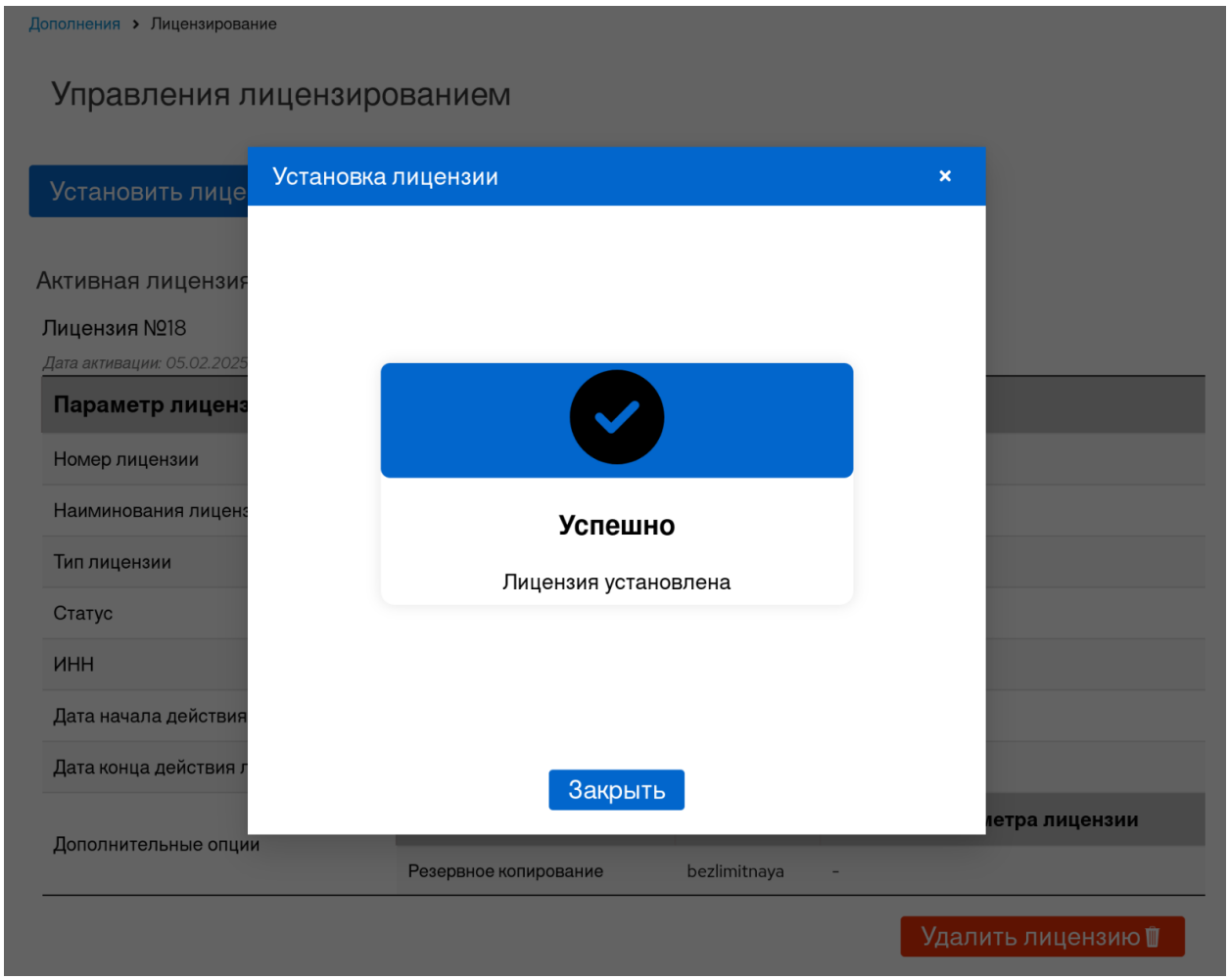

Рисунок 76 – Подтверждение успешности загрузки лицензии

г) нажать на кнопку Закрыть (рисунок 76).

Действия, описанные выше, применяются при установке новой или расширяющей лицензии.

Если устанавливается лицензия с пересечением сроков действия с текущей лицензией, отобразится сообщение с предупреждением в меню установки. В данном предупреждении будут описаны сроки действия лицензий. В случае согласия устанавливается новая лицензия с сообщениями об успехе или об ошибке.

3.7.1.3 Работа с лицензиями

В результате установки лицензии откроется окно управления лицензированием с информацией об установленной лицензии (рисунок 77).

Неактивные лицензии можно сортировать, чтобы посмотреть будущие и просроченные лицензии. Рекомендуется удалять просроченные лицензии.

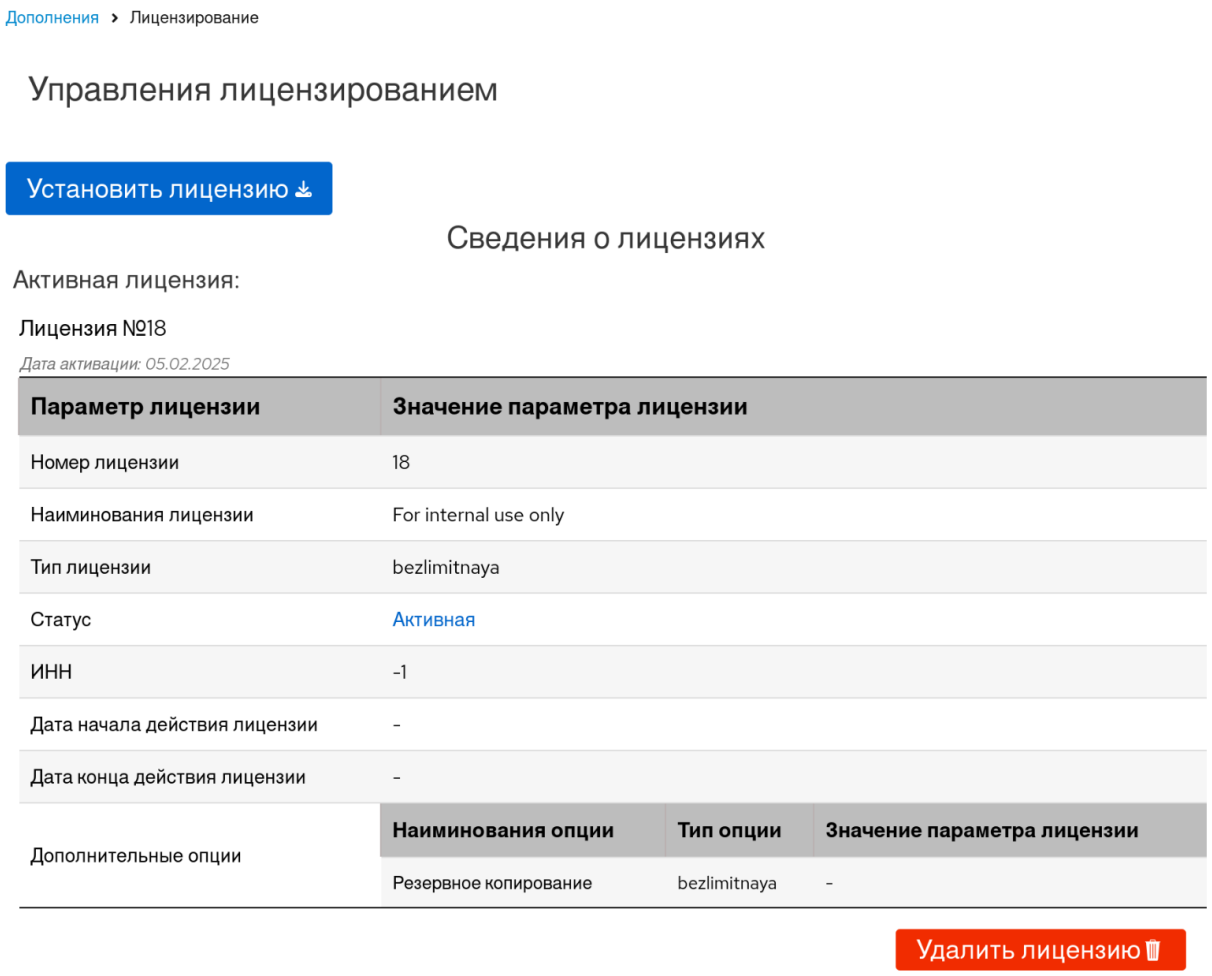

Рисунок 77 – Информация об установленной лицензии в веб-интерфейсе

При необходимости удаления лицензии и установки другой лицензии нужно нажать на кнопку `Удалить лицензию`, в диалоговом окне подтвердить удаление, нажав на кнопку `Удалить`, или отменить удаление, нажав на кнопку `Отменить`.

После успешного удаления лицензий в диалоговом окне появится сообщение "Успешно". Если возникла ошибка, то появится сообщение об ошибке.

3.7.2 Активация лицензии POCA Виртуализация через интерфейс CLI

Для активации лицензии POCA Виртуализация через интерфейс CLI нужно:

а) подключиться к консоли СУСВ по SSH или открыть терминал в веб-интерфейсе администрирования хоста;

б) скопировать файл с лицензией РОСА Виртуализация в один из каталогов ВМ СУСВ (например, /tmp). Для копирования можно использовать утилиту SCP (Secure Copy Protocol) или аналогичную ей;

Примечание – Для подключения к консоли СУСВ по SSH нужно выполнить 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:
```

в) выполнить активацию лицензии РОСА Виртуализация утилитой install-rosa-license в консоли СУСВ:

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

г) при выводе на экран соответствующего запроса ввести путь к файлу с лицензией.

Далее интерактивный сценарий автоматически осуществит активацию лицензии РОСА Виртуализация.

3.7.2.1 Пример активации лицензии РОСА Виртуализация

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

```
[root@susv ~]# install-rosa-license
Path to POCA Виртуализация 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.

3.7.2.2 Пример просмотра информации об лицензии

Для просмотра подробной информации и проверки валидности установленной лицензии можно выполнить в консоли СУСВ следующую команду:

```
# rosa-license-info
[root@susv ~]# rosa-license-info
```

```
VM_Backup appliance is allowed: 1.
ROSA license is valid.
```

В данном примере лицензия верифицирована. Для операций резервного копирования можно использовать один клиент (Backup Appliance).

3.8 Установка сервера IPA

В составе РОСА Виртуализация 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 РОСА Виртуализация.

Для установки сервера IPA на ВМ под управлением РОСА Виртуализация необходимо предварительно создать новую ВМ на Портале администрирования СУСВ, а также загрузить образ с дистрибутивом (файл RV-4.0-20260116.0-rv-x86_64-dvd1.iso) в хранилище в подкаталог /iso.

Для установки сервера IPA на отдельный физический сервер используется DVD с дистрибутивом РОСА Виртуализация 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 необходимо:

а) авторизоваться на Портале администрирования СУСВ. На экране появится интерфейс Портала администрирования с главным меню СУСВ;

б) в главном меню СУСВ выбрать пункт "Ресурсы → Виртуальные машины" и нажать кнопку Добавить. На экране появится вкладка "Общие" окна "Новая ВМ" (рисунок 78);

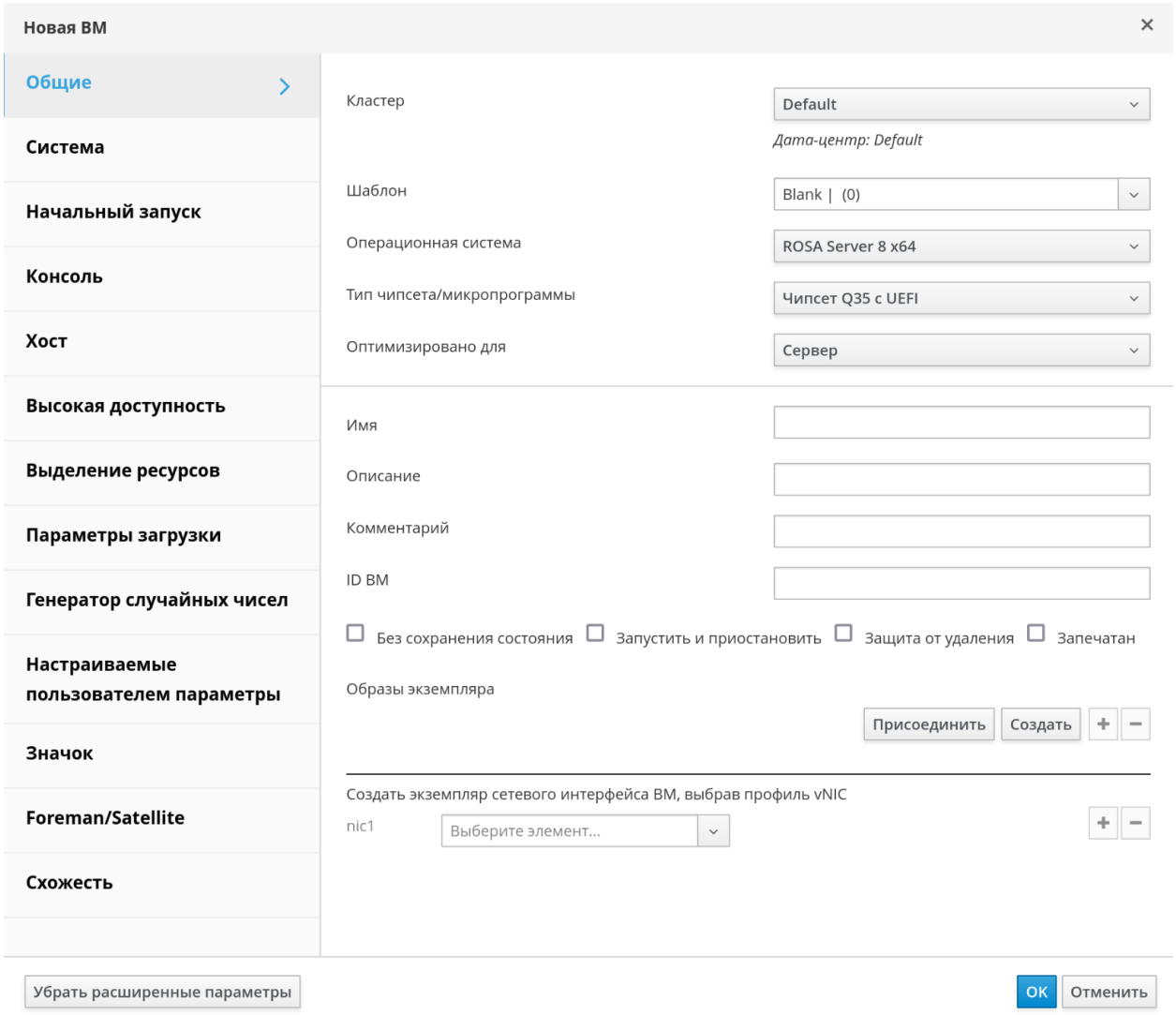

Рисунок 78 – Вкладка "Общие" окна "Новая ВМ"для создания новой виртуальной машины

в) в поле "Имя" ввести уникальное наименование для новой ВМ (например, "Server-IPA");

г) для создания виртуального диска ВМ нажать кнопку Создать. На экране появится окно "Новый виртуальный диск" (рисунок 79);

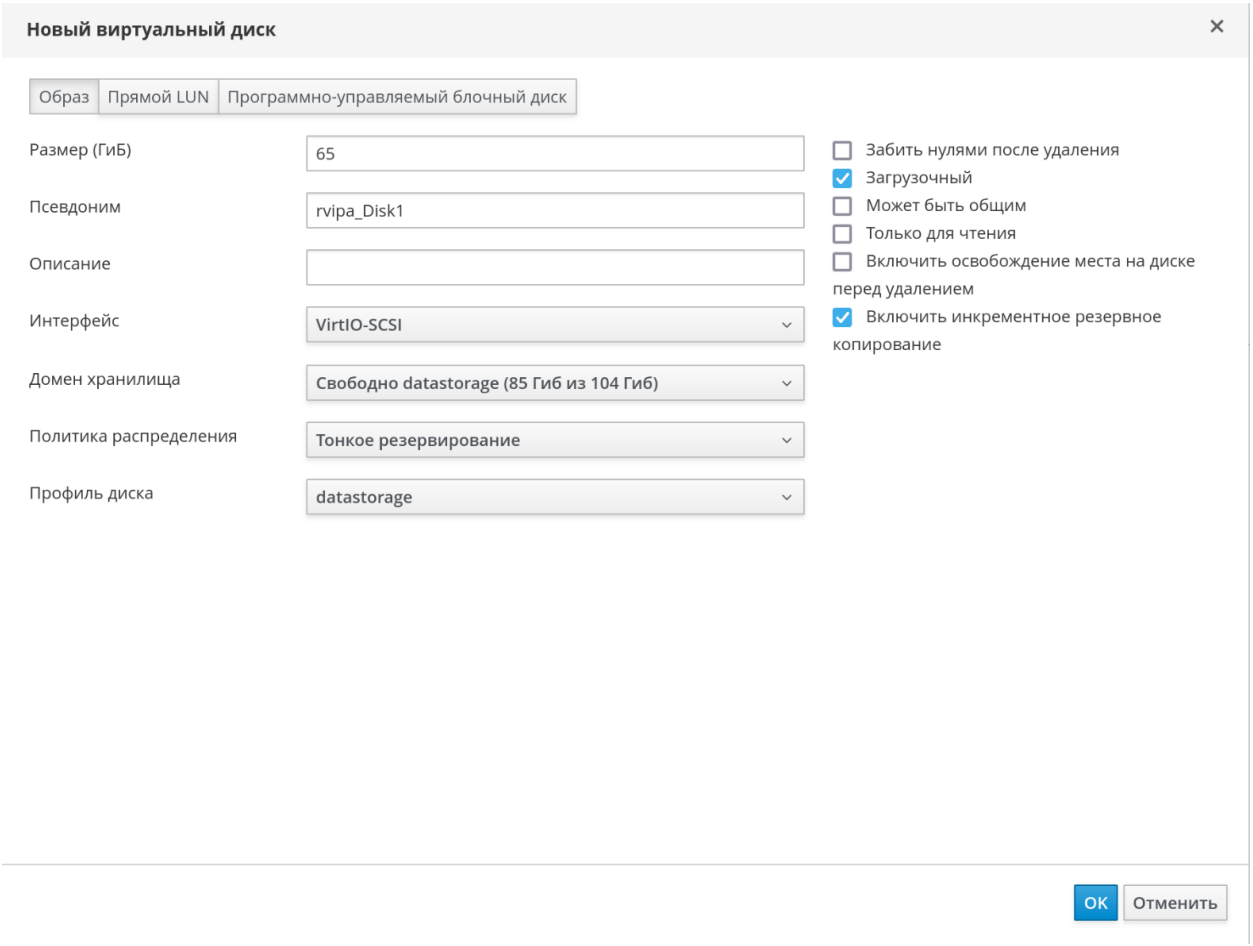

Рисунок 79 – Окно "Новый виртуальный диск"

д) в поле "Размер (ГиБ)" указать размер виртуального диска не менее 62 ГБ;

е) после настройки опциональных параметров виртуального диска нажать кнопку OK для сохранения указанных значений и возвращения в окно "Новая ВМ";

ж) в окне "Новая ВМ" перейти на вкладку "Система" (рисунок 80);

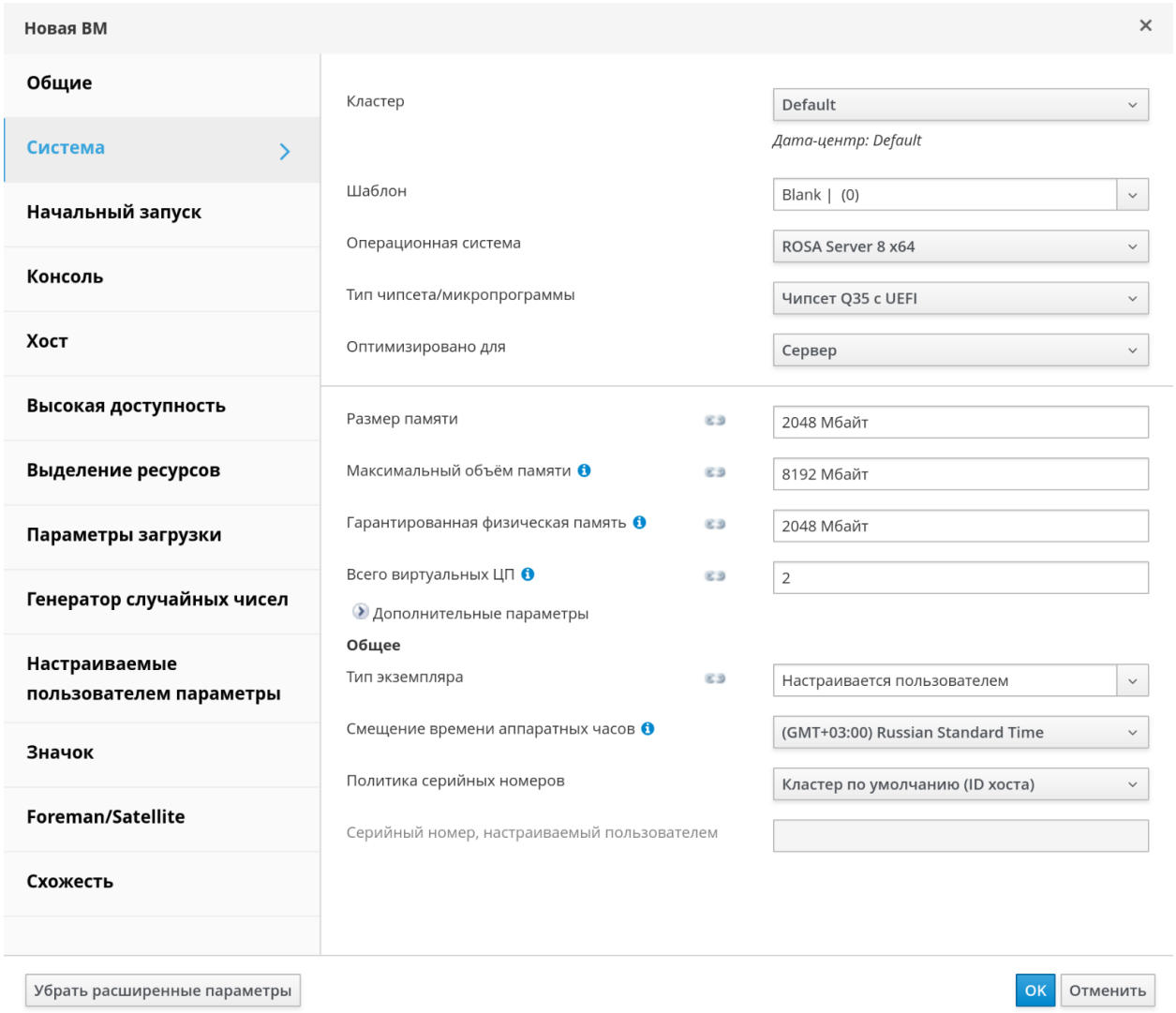

Рисунок 80 – Вкладка "Система"

з) в поле "Размер памяти" указать объем используемой оперативной памяти не менее 2 ГБ. В поле "Всего виртуальных ЦП" указать требуемое число виртуальных процессоров (ядер) (рисунок 80);

и) выбрать региональные настройки;

к) перейти на вкладку "Параметры загрузки" (рисунок 81);

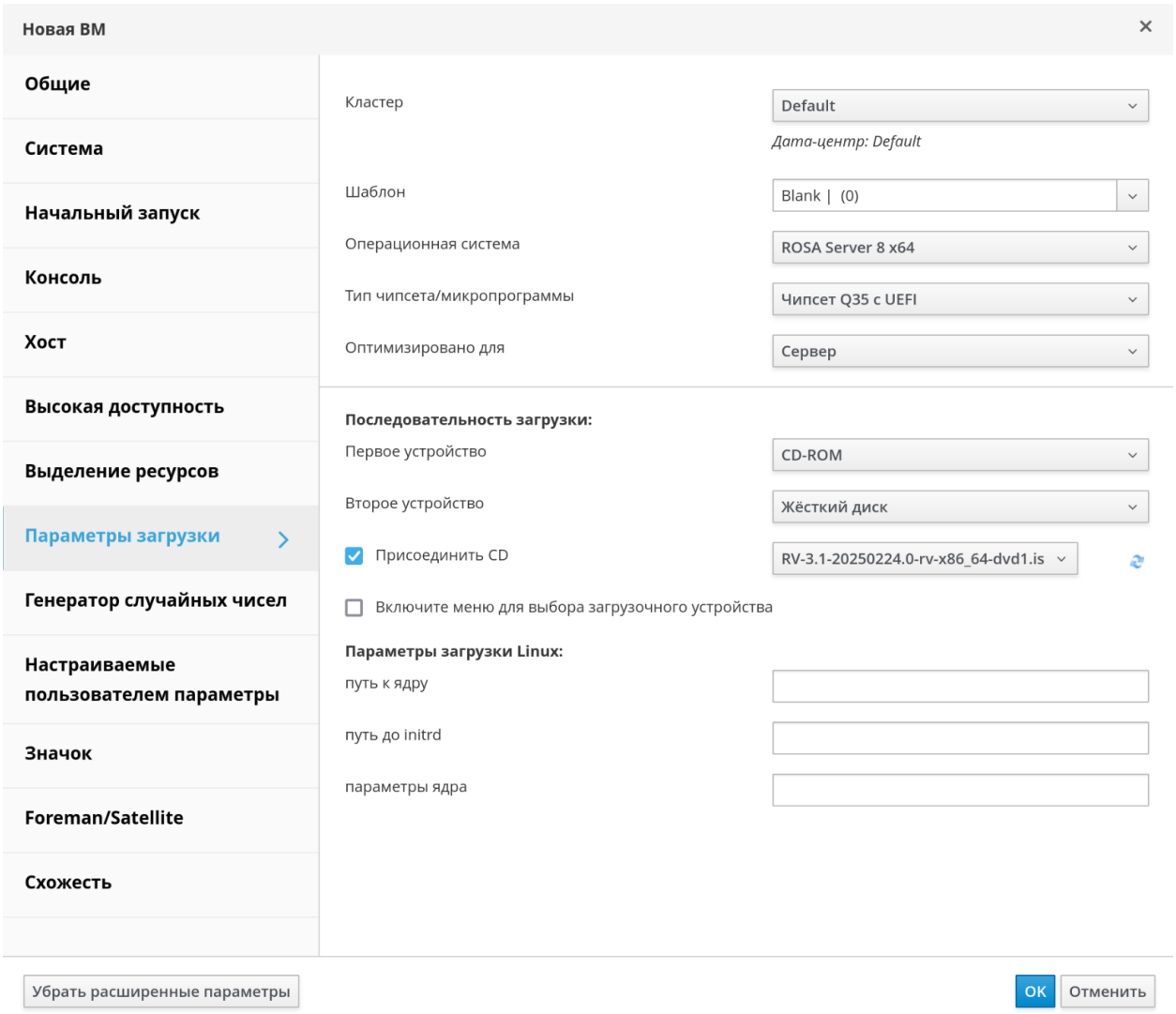

Рисунок 81 – Вкладка "Параметры загрузки"

л) установить последовательность загрузки устройств. Для последующей установки ОС с загруженного образа с дистрибутивом сервера IPA выбрать из выпадающего списка "Первое устройство" значение "CD-ROM", а из выпадающего списка "Второе устройство" значение "Жесткий диск" (рисунок 81);

м) установить флажок "Присоединить CD" и выбрать из выпадающего списка образ с дистрибутивом (файл RV-4.0-20260116.0-rv-x86_64-dvd1.iso);

н) для применения всех сделанных настроек и создания новой ВМ нажать кнопку OK;

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

После создания новой ВМ требуется настроить параметры виртуального сетевого интерфейса. Для этого во внутреннем меню ВМ нужно нажать кнопку

Изменить и во вкладке "Общие" выбрать из выпадающего списка необходимое значение (рекомендуемый вариант – "ovirtmgmt").

Для перехода к процессу установки ОС на сервер IPA следует выбрать созданную ВМ и нажать кнопку Запустить, а после изменения состояния ВМ нажать 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 необходимо загрузить физический сервер или созданную ВМ с носителя с дистрибутивом сервера IPA.

На экране последовательно появятся меню программы установки, окно приветствия и меню "Обзор установки", которое содержит различные секции для настройки параметров установки (рисунок 82).

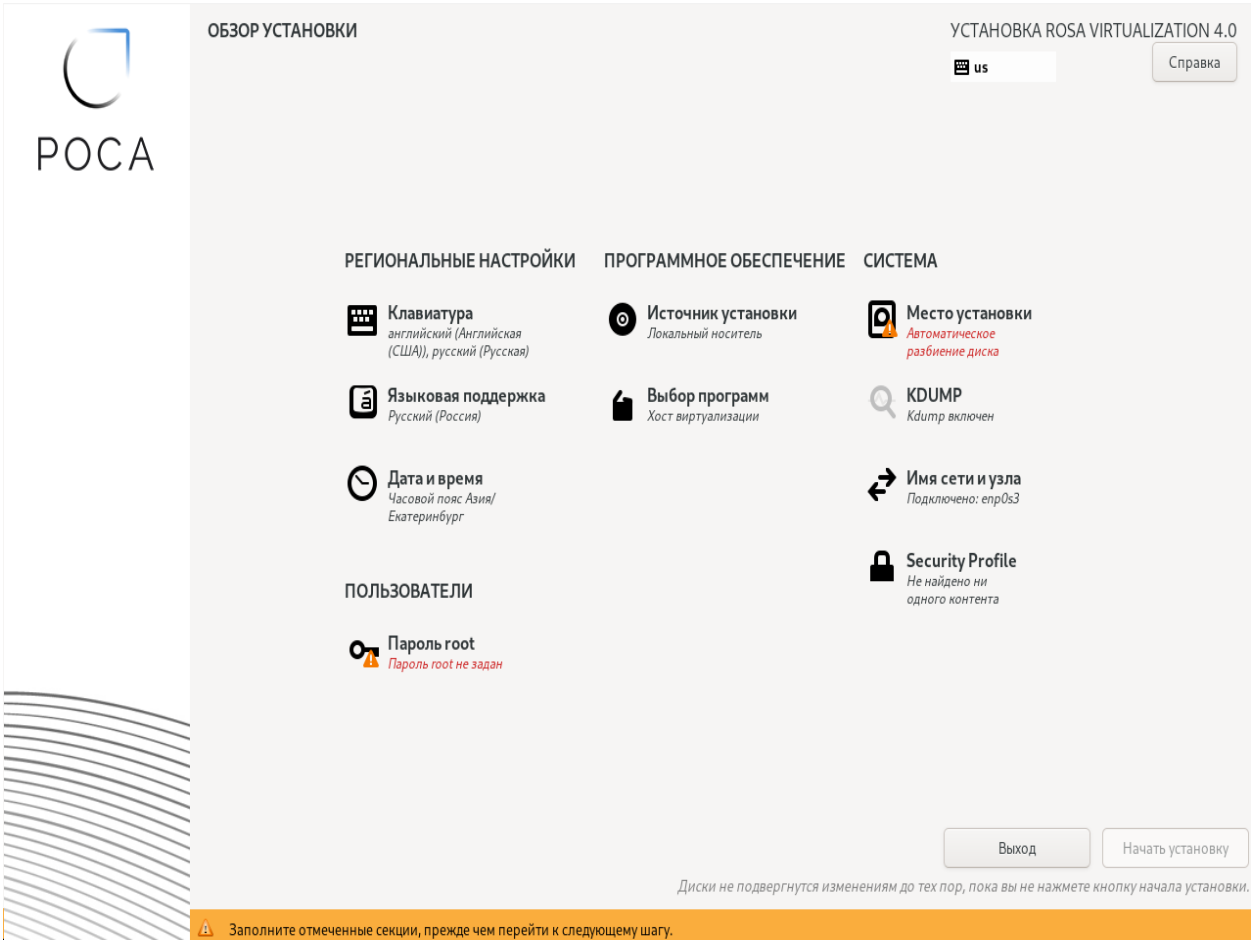

Рисунок 82 – Обзор установки РОСА Виртуализация

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

Для перехода к интерфейсу настройки соответствующих параметров следует нажимать на наименования секций. После настройки параметров нужно нажать кнопку Готово для возвращения в меню "Обзор установки".

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

– Выбор программ;
– Место установки;
– Имя сети и узла;
– Пароль root.

В секции "Выбор программ" необходимо установить переключатель "Базовое окружение" в положение "Служба каталогов (РОСА Функции контроллера домена)" (рисунок 83) для установки соответствующего базового ПО в систему.

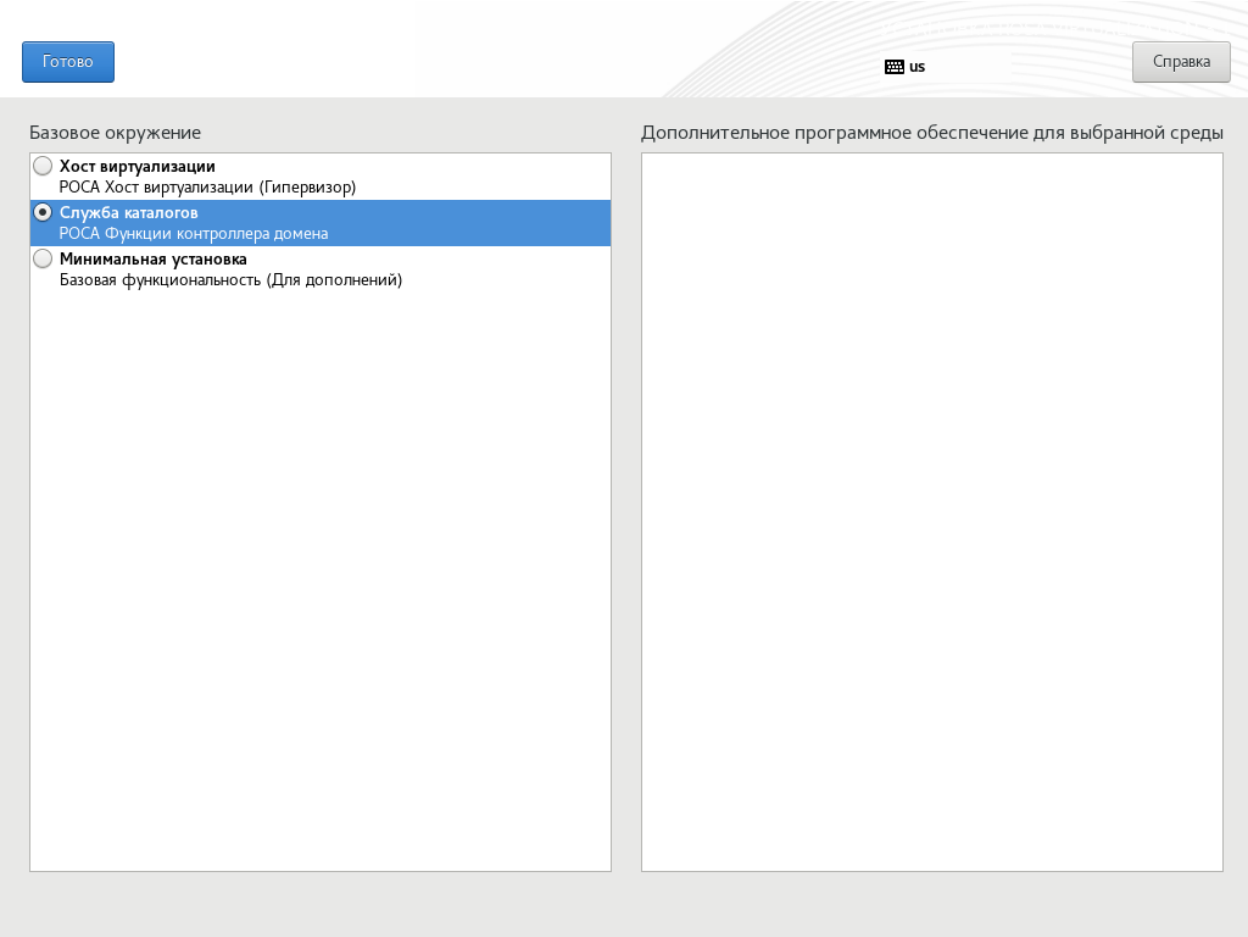

Рисунок 83 – Выбор базового ПО для установки: "Служба каталогов – РОСА Функции контроллера домена"

В секции "Место установки" нужно выбрать необходимый диск и установить переключатель "Конфигурация устройств хранения" в положение "Автоматически".

В секции "Имя сети и узла" следует задать полное доменное имя сервера IPA (например, ipa.rosa.lan), подключить необходимый сетевой интерфейс и настроить параметры сетевого соединения: DHCP или статические значения IP-адреса (например, 10.10.20.8), маску сети (255.255.255.0), шлюз по умолчанию (10.10.20.1) и сервер DNS (10.10.20.1).

В секции "Пароль root" нужно установить пароль для учетной записи суперпользователя root.

После настройки всех обязательных параметров необходимо нажать кнопку `Начать установку` для старта процесса установки ОС (рисунок 82).

После завершения процесса установки необходимо нажать кнопку `Перезагрузка системы` (рисунок 84).

Рисунок 84 – Окно с информацией о завершении установки системы и кнопкой перезагрузки системы

Далее на физическом сервере следует извлечь DVD или USB-накопитель, с которого выполнялась установка, а в настройках ВМ установить 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 85).

Рисунок 85 – 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

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

3.8.3.2 Запуск сценария установки сервера IPA

Для запуска интерактивного сценария установки сервера IPA необходимо:

а) осуществить вход в систему от имени учетной записи суперпользователя root и выполнить 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.

б) для подтверждения согласия на настройку встроенной службы DNS ввести "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]:
```

в) чтобы принять предложенные значения по умолчанию, нажать клавишу `Enter`;

г) при необходимости можно внести изменения в имя хоста сервера, имя домена, имя области Kerberos, соответствующие установке в актуальном ЦОД, и затем нажать 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.

д) установить (ввести и подтвердить) 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):
```

е) сценарий установки предложит настроить перенаправление DNS:

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

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

Для настройки перенаправления DNS нажать клавишу `Enter` или ввести "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.

ж) сценарий установки предложит проверить, нужно ли настроить какие-либо обратные записи DNS для IP-адресов, связанных с сервером IPA. Для подтверждения нажать клавишу `Enter` или ввести "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 нажать 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.
```

з) сценарий установки предложит настроить доменное имя NetBIOS. Ввести доменное имя NetBIOS, для подтверждения нажать клавишу `Enter`:

```
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]:
```

и) опционально можно 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]:
```

к) сценарий установки выведет в консоль выбранные параметры настройки сервера IPA. Проверить указанные настройки на соответствие требуемым:

```
    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 ввести "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 кеширует начальный билет на выдачу билетов для принципала.

Для получения билета Kerberos для учетной записи администратора admin нужно выполнить в консоли сервера IPA команду:

```
# kinit 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 используют 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. При этом 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 можно 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 используют 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 запрос:

```
Пароль:
```

в котором необходимо указать требуемый (желаемый) пароль пользователя.

Затем появится запрос:

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

и в нем 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 используют команду:

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

где "user_name" – это имя пользователя:

Следует указать "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="2025-09-01
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: 202509031200002
```

```
  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 – 2025-09-01 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" используют команду:

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

где "user_name" – это имя пользователя.

Следует указаь "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 используют 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 используют 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 нужно выполнить 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 требуемых портов сервера IPA в зоне "default" службы межсетевого экрана firewalld нужно выполнить 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

Примечание – Не следует беспокоиться о том, что сервер IPA использует порты 80 и 389:

– 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);

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

Для применения изменений необходимо перезагрузить конфигурацию межсетевого экрана, выполнив 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 можно выполнить 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 2025-01-01 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 необходимо ввести 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 86).

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
```

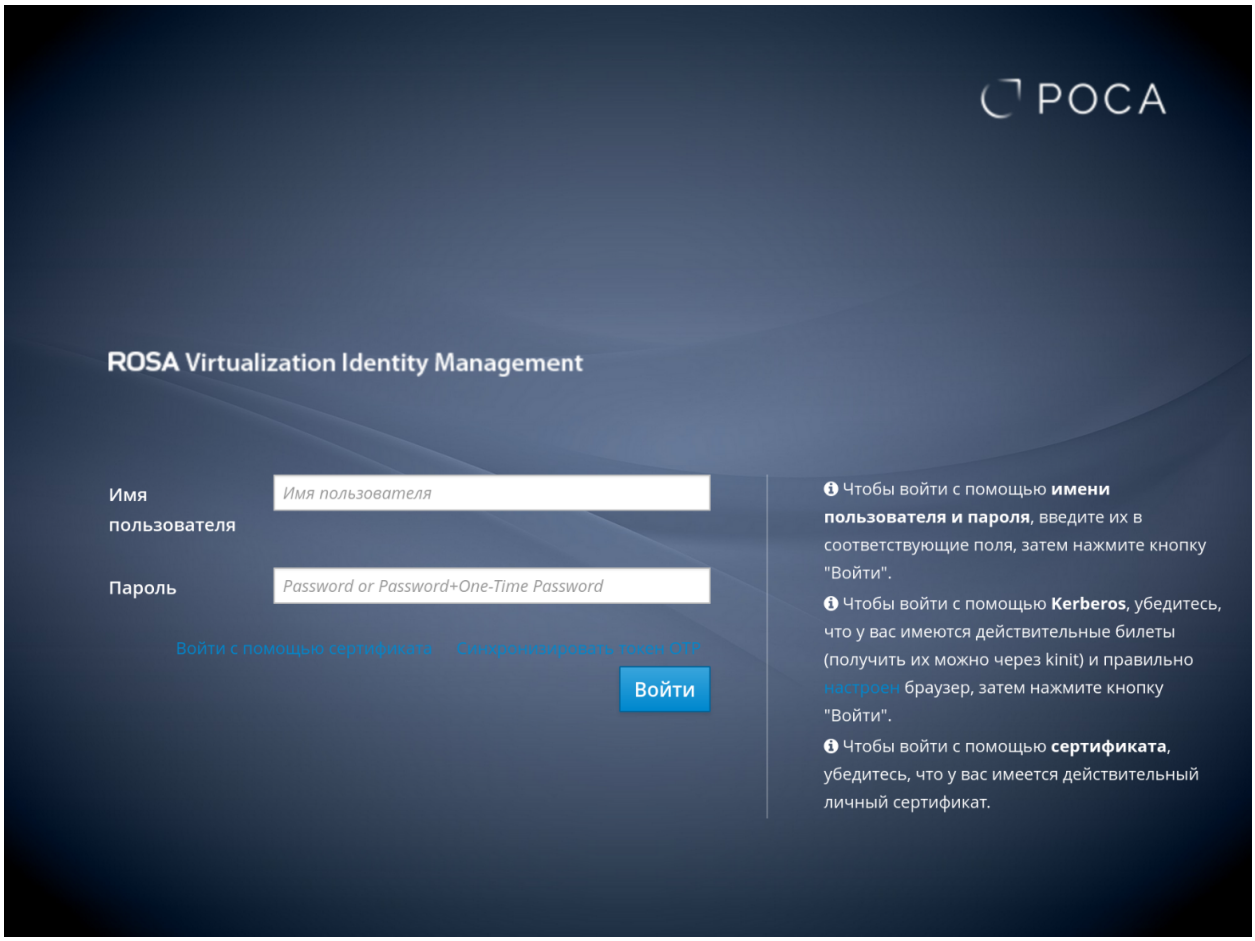

Рисунок 86 – Окно авторизации интерфейса управления сервером IPA

Для входа в интерфейс нужно ввести имя (логин) и пароль пользователя в соответствующие поля, после чего нажать кнопку Войти.

После входа в веб-интерфейс сервера IPA будет отображена панель управления сервером IPA. По умолчанию будет открыта вкладка "Идентификация → Активные пользователи" (рисунок 87).

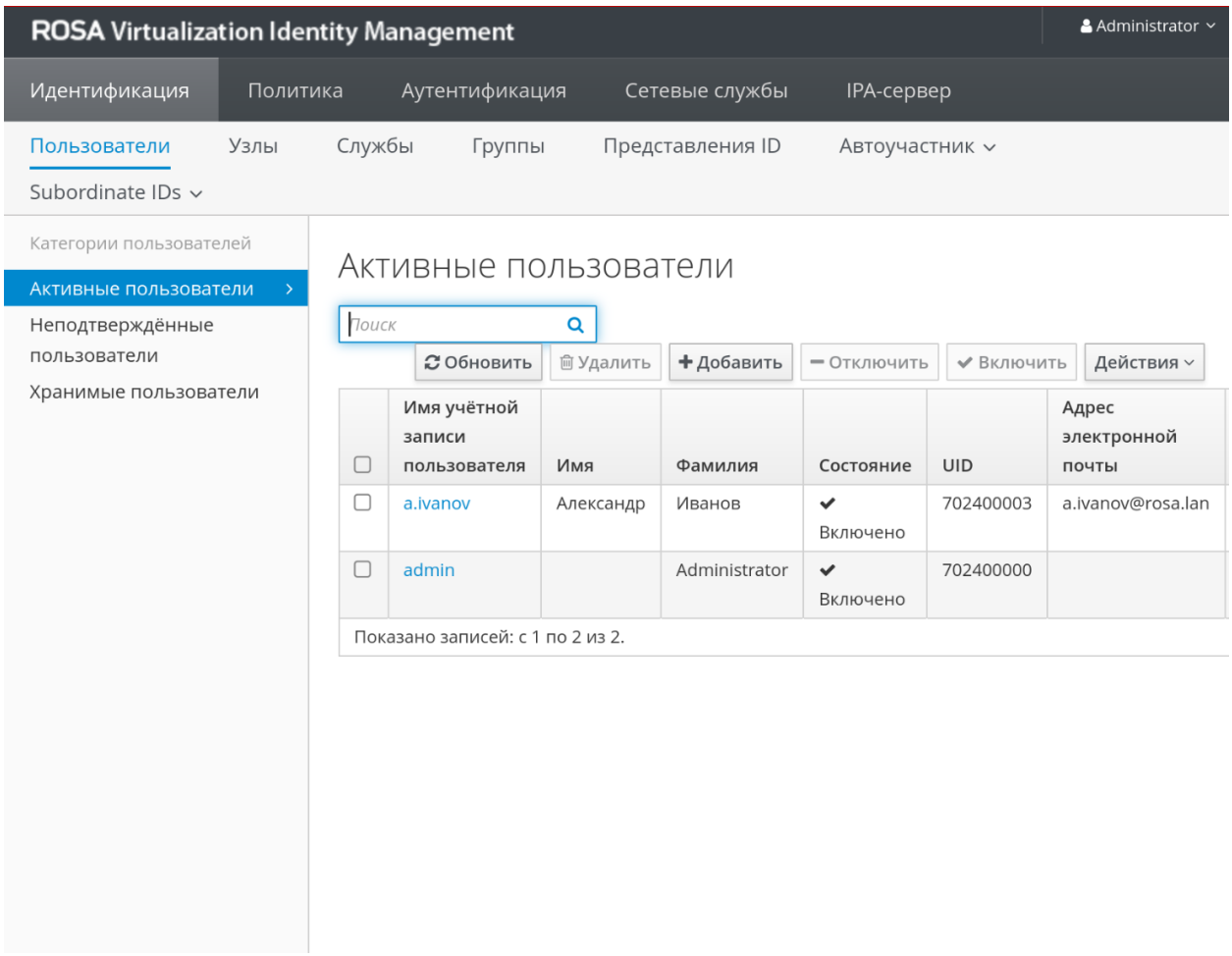

Рисунок 87 – Веб-интерфейс сервера IPA – вкладка "Идентификация" → "Активные пользователи"

Если ранее какие-либо пользователи уже были добавлены в каталог IPA, используя интерфейс командной строки, то эти пользователи будут отображены с списке активных пользователей.

3.9 Подключение РОСА Виртуализация к службе каталогов LDAP сервера IPA

Процедура подключения РОСА Виртуализация 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 системной 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 системной учетной записи пользователя с использованием веб-интерфейса

Модуль "Системный пользователь" является частью интерфейса РОСА Виртуализация и устанавливается из отдельного дистрибутива.

Для перехода в раздел "Системный пользователь" необходимо в навигационном меню выбрать пункт "Дополнения → Настройки", после чего откроется окно , в котором открыть вкладку "Системный пользователь". В результате отобразится интерфейс модуля "Системный пользователь" (рисунок 88).

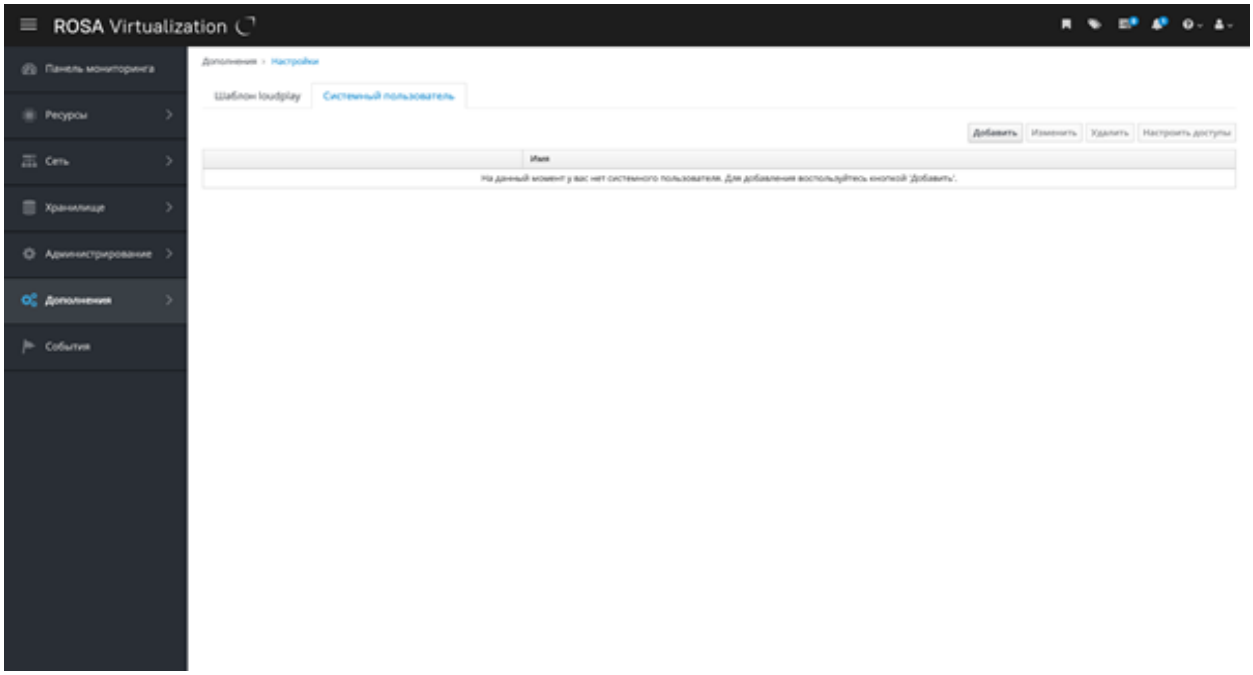

Рисунок 88 – Вкладка "Системный пользователь"

Основные функции модуля:

– Отображение активного системного пользователя со статусом валидности его данных.
– Добавление пользователя.
– Изменение данных пользователя.
– Удаление пользователя.
– Выдача прав доступа сервисам.

3.9.1.1 Отображение активного системного пользователя

В окне модуля "Системный пользователь" отображается единственный активный системный пользователь (рисунок 89). Слева от имени пользователя отображается индикатор статуса валидности данных:

– Зелёный треугольник — пользователь валиден, данные корректны;

– Красный треугольник — пользователь невалиден (например, изменились логин или пароль в системе аутентификации).

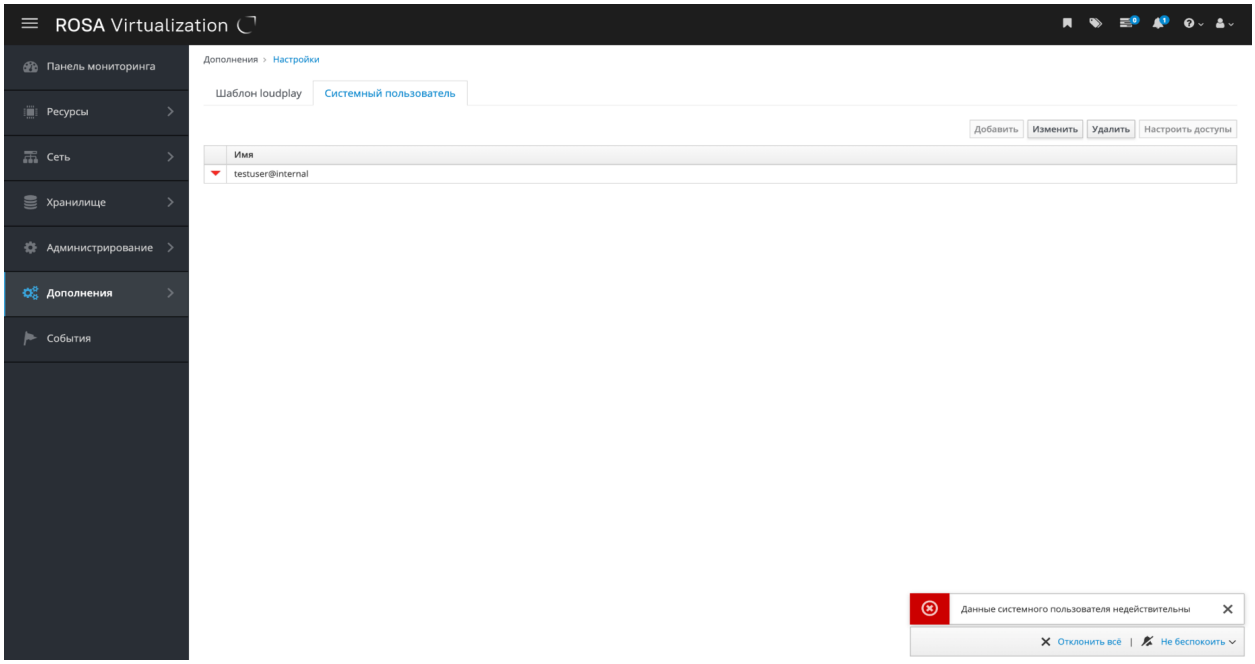

Рисунок 89 – Отображение системного пользователя

Статус пользователя может изменяться автоматически в зависимости от актуальности сохранённых данных.

Если данные становятся невалидными, в правом нижнем углу интерфейса отображается уведомление о необходимости обновить информацию системного пользователя.

В случае появления красного треугольника и уведомления рекомендуется нажать кнопку Изменить, чтобы обновить данные пользователя (логин или пароль) либо удалить текущего пользователя и добавить нового с актуальными данными.

3.9.1.2 Добавление системного пользователя

Для добавления нового системного пользователя нужно нажать кнопку "Добавить" и в открывшемся окне (рисунок 90) в полях:

– Имя – ввести полное имя вместе с профилем, например admin@internal или user@internalsso;

– Пароль – указать действительный пароль для выбранного пользователя.

После ввода данных следует нажать кнопку Добавить.

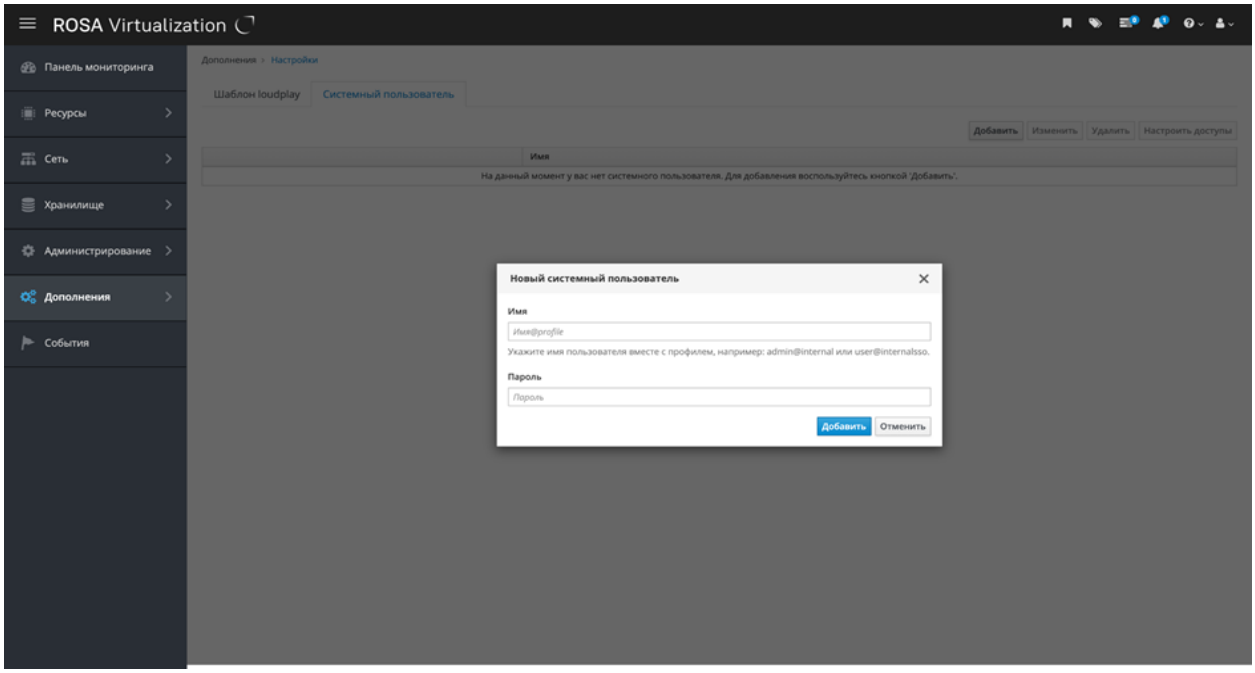

Рисунок 90 – Добавление системного пользователя

Если данные введены корректно, пользователь успешно добавляется в Систему, отображается уведомление о добавлении, а новый пользователь появляется в таблице (рисунок 91).

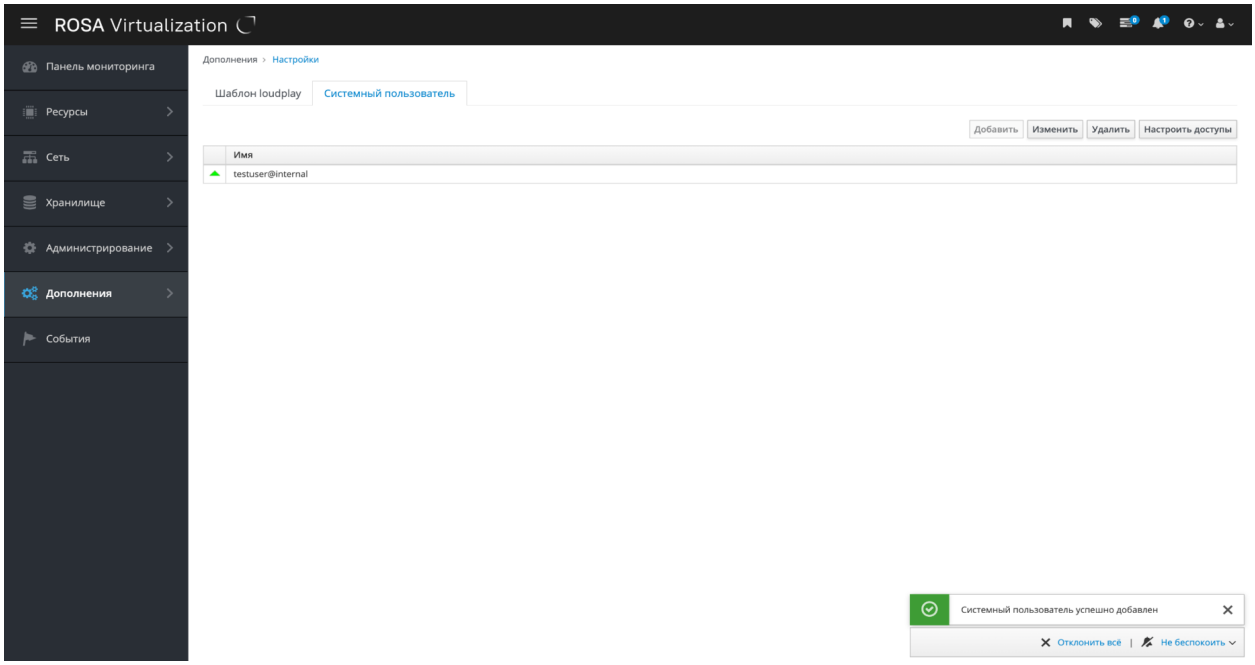

Рисунок 91 – Добавленный системный пользователь

Если введены некорректные данные (например, неверное имя пользователя или пароль), в форме появится сообщение об ошибке "Неверное имя пользователя или пароль".(рисунок 92)

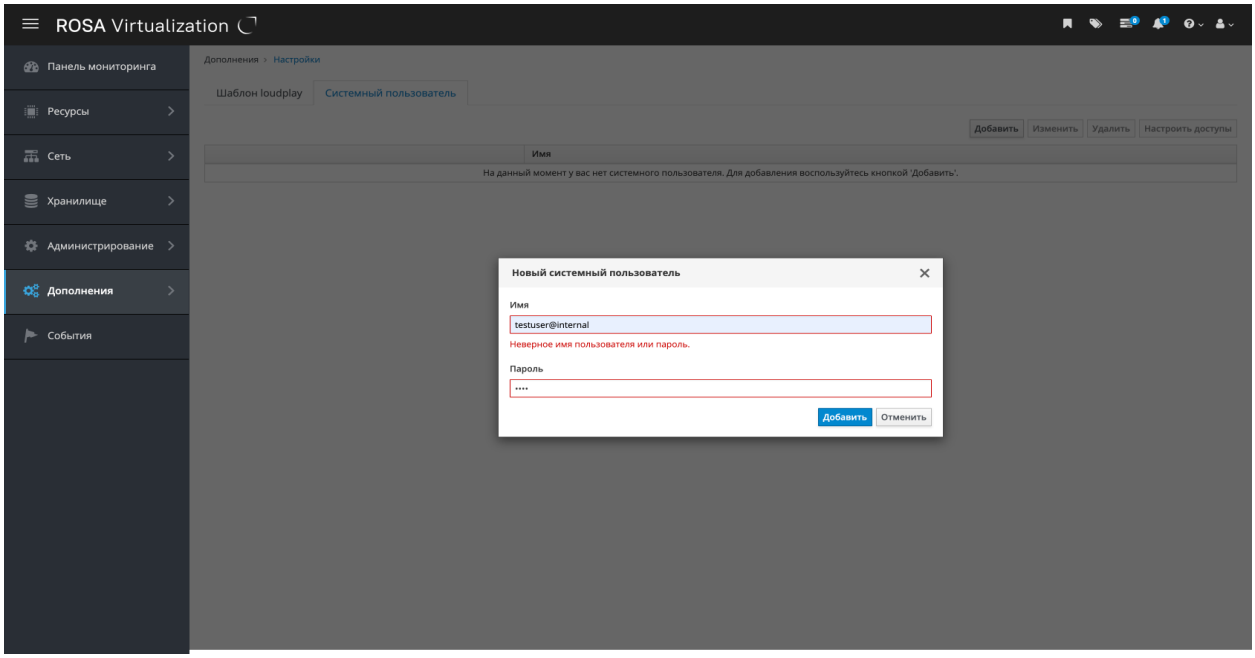

Рисунок 92 – Сообщение об ошибке

3.9.1.3 Изменение данных системного пользователя

Для изменения данных системного пользователя нужно нажать кнопку Изменить, откроется форма, аналогичная форме добавления пользователя (рисунок 93).

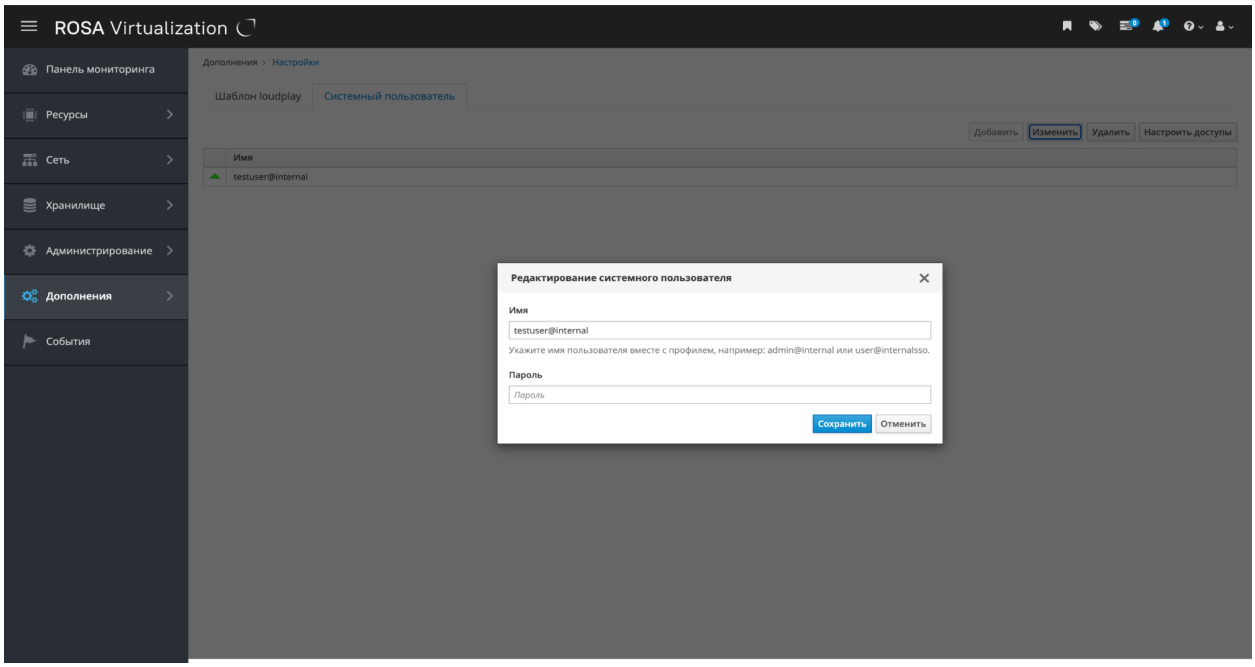

Рисунок 93 – Изменение данных пользователя

Поле "Имя" заполняется автоматически и содержит текущее имя пользователя.

При необходимости можно обновить только пароль или оба поля. После внесения изменений следует нажать кнопку Сохранить. Если введённые данные корректны, появится уведомление об успешном изменении, а статус пользователя обновится в таблице (рисунок 94).

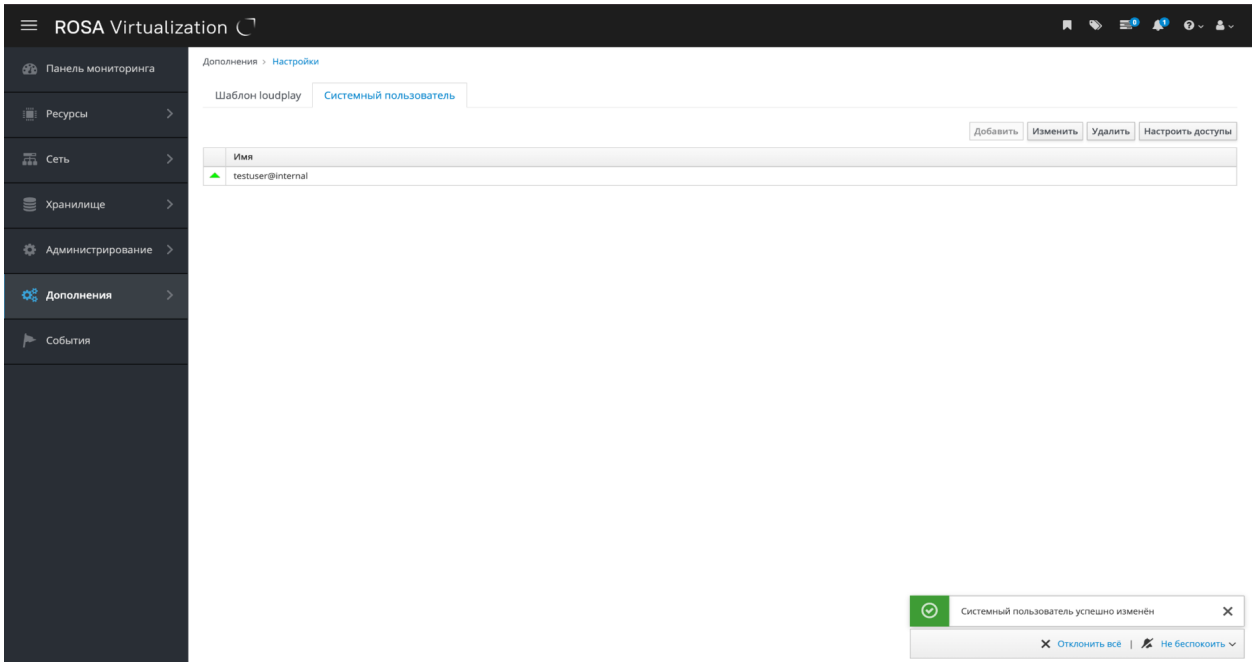

Рисунок 94 – Обновленные данные пользователя

Если данные невалидны (например, указан неверный логин или пароль), в форме появится сообщение об ошибке "Неверное имя пользователя или пароль".

3.9.1.4 Удаление пользователя

Для удаления системного пользователя нужно нажать кнопку Удалить. В результате откроется диалоговое окно с подтверждением действия (рисунок 95).

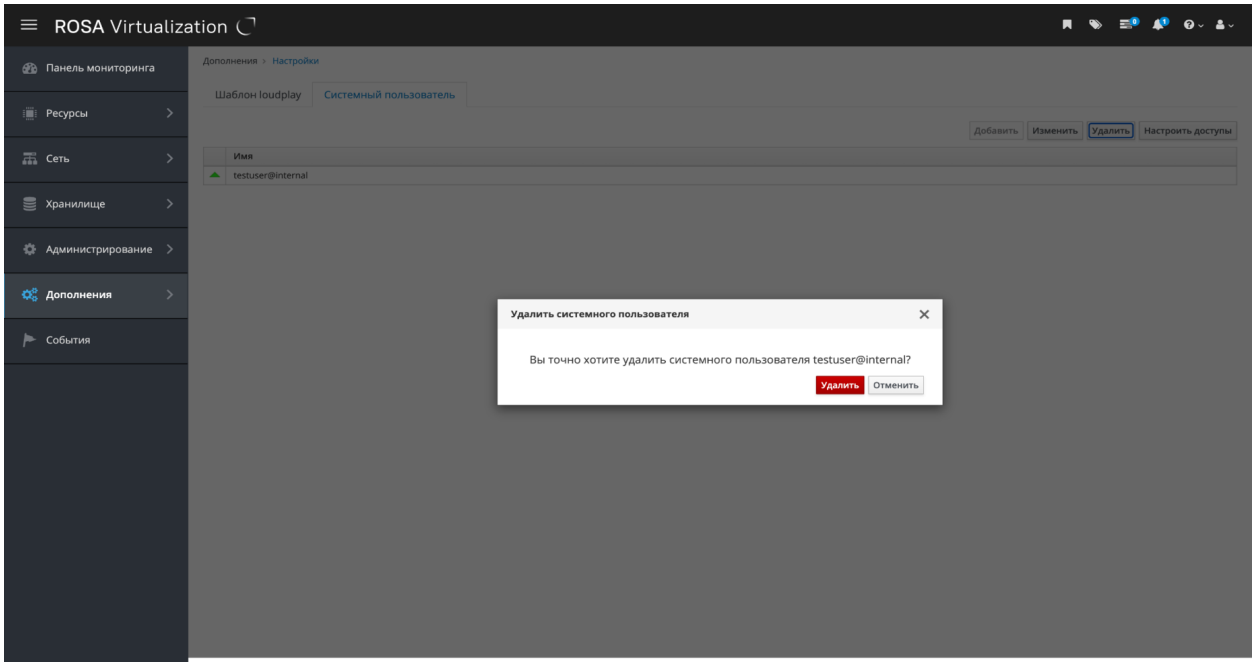

Рисунок 95 – Подтверждение удаления пользователя

При подтверждении действия по кнопке Удалить пользователь будет удален из Системы и из таблицы отображения. После успешного удаления появится уведомление о том, что пользователь удалён (рисунок 96).

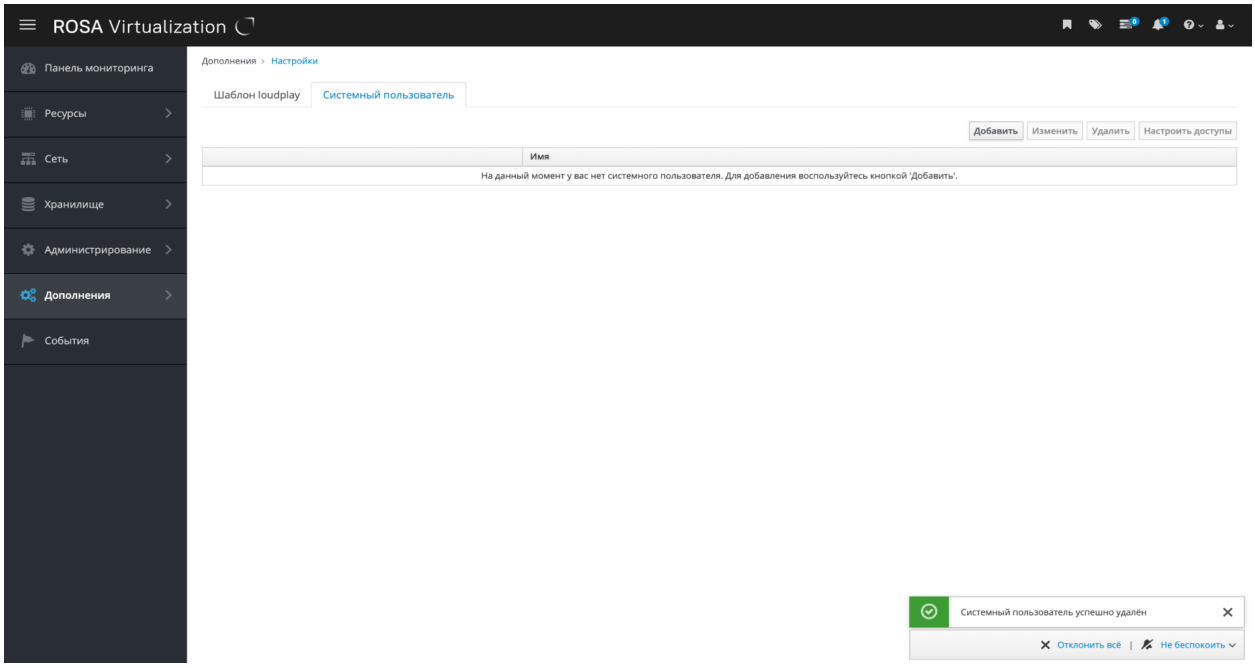

Рисунок 96 – Сообщение об успешном удалении

3.9.1.5 Выдача прав доступа сервисам

Для настройки прав доступа нужно нажать кнопку Настроить доступы.

В открывшемся окне "Настройка доступа сервисов" отображается таблица со списком всех доступных сервисов, которым можно выдать или отозвать доступ (рисунок 97).

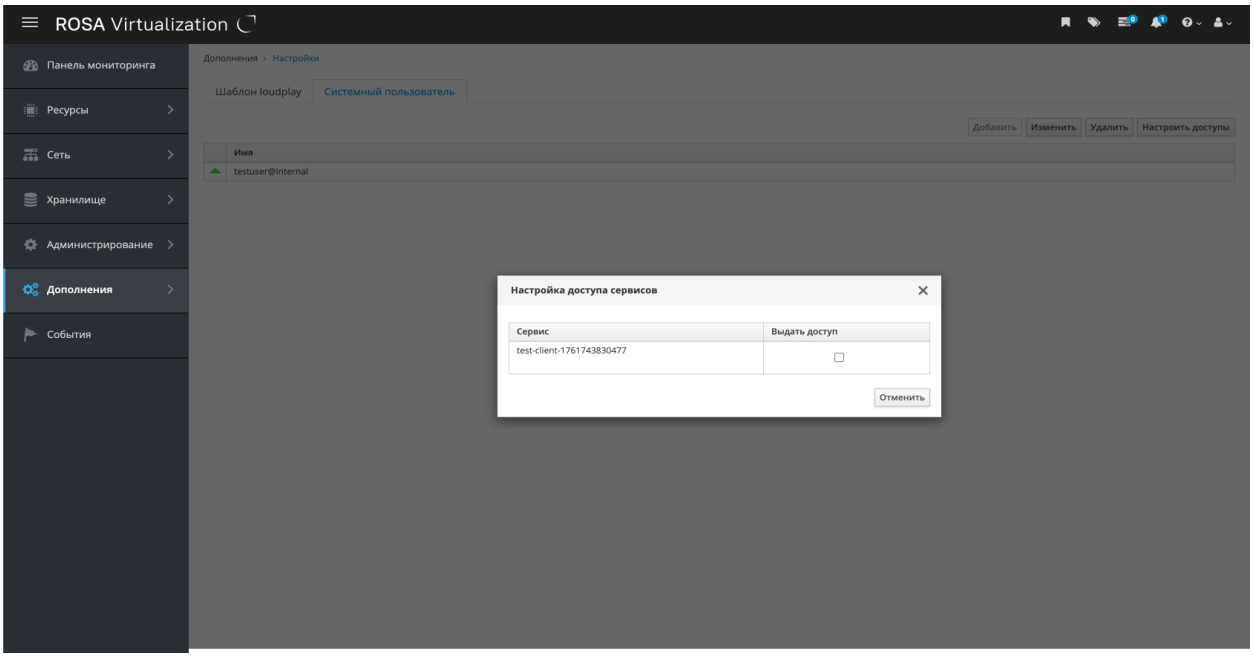

Рисунок 97 – Окно "Настройка доступа сервисов"

В таблице для каждого сервиса предусмотрен флажок в столбце "Выдать доступ":

– если установить флажок, выбранному сервису выдаётся доступ;
– если снять флажок, доступ для данного сервиса отзывается.

После выполнения действия отображается уведомление о результате операции:

– при выдаче доступа — уведомление "Права доступа успешно выданы" (рисунок 98);
– при отзыве доступа — уведомление "Права доступа отозваны" (рисунок 99).

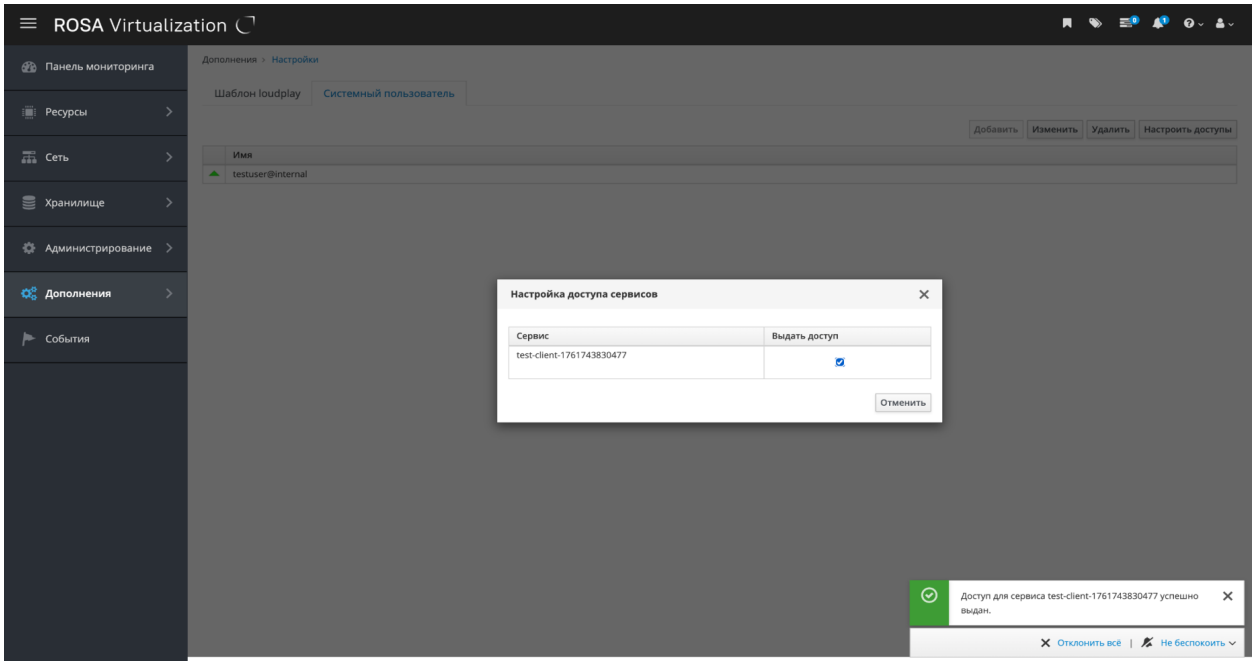

Рисунок 98 – Доступ выдан

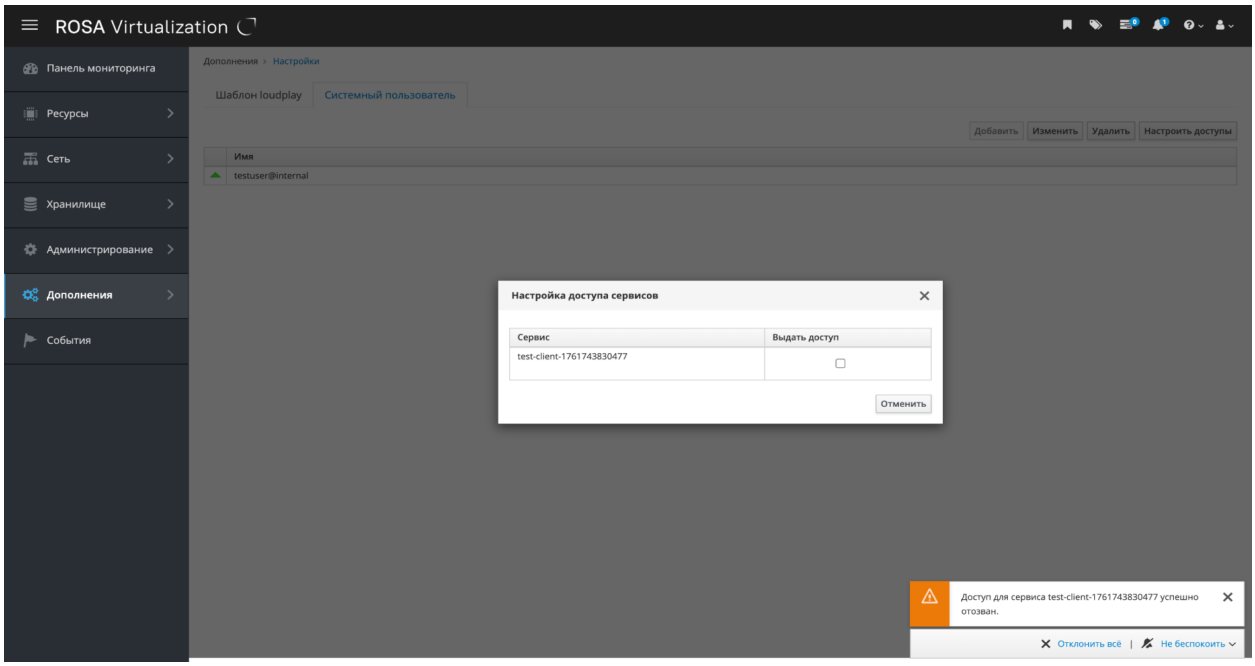

Рисунок 99 – Доступ отозван

3.9.2 Создание профиля подключения к службе каталогов LDAP с помощью веб-интерфейса

Плагин "Мастер настройки LDAP" являются частью интерфейса РОСА Виртуализация и устанавливается из отдельного дистрибутива.

Для настройки профиля подключения СУСВ к службе каталогов LDAP с помощью веб-интерфейса нужно перейти в раздел "Дополнения → Мастер настройки LDAP" (рисунок 100).

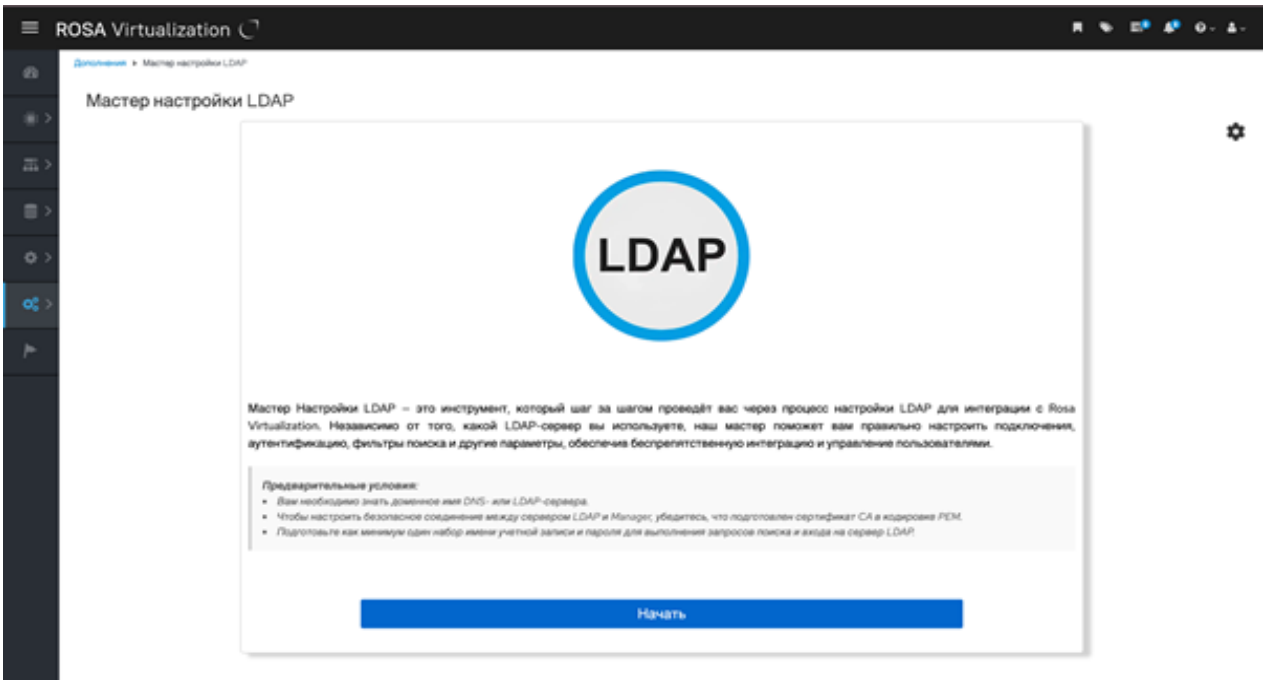

Рисунок 100 – Мастер настройки LDAP в административной панели СУСВ

Для начала работы с "Мастером настройки LDAP" нужно нажать на кнопку Начать и выполнить следующие действия:

а) выбрать реализацию LDAP, которая планируется к использованию, например OpenLDAP, Microsoft Active Directory или другой LDAP-сервер, и настроить параметры подключения, включая DNS и протоколы, используемые для связи с сервером (рисунок 101);

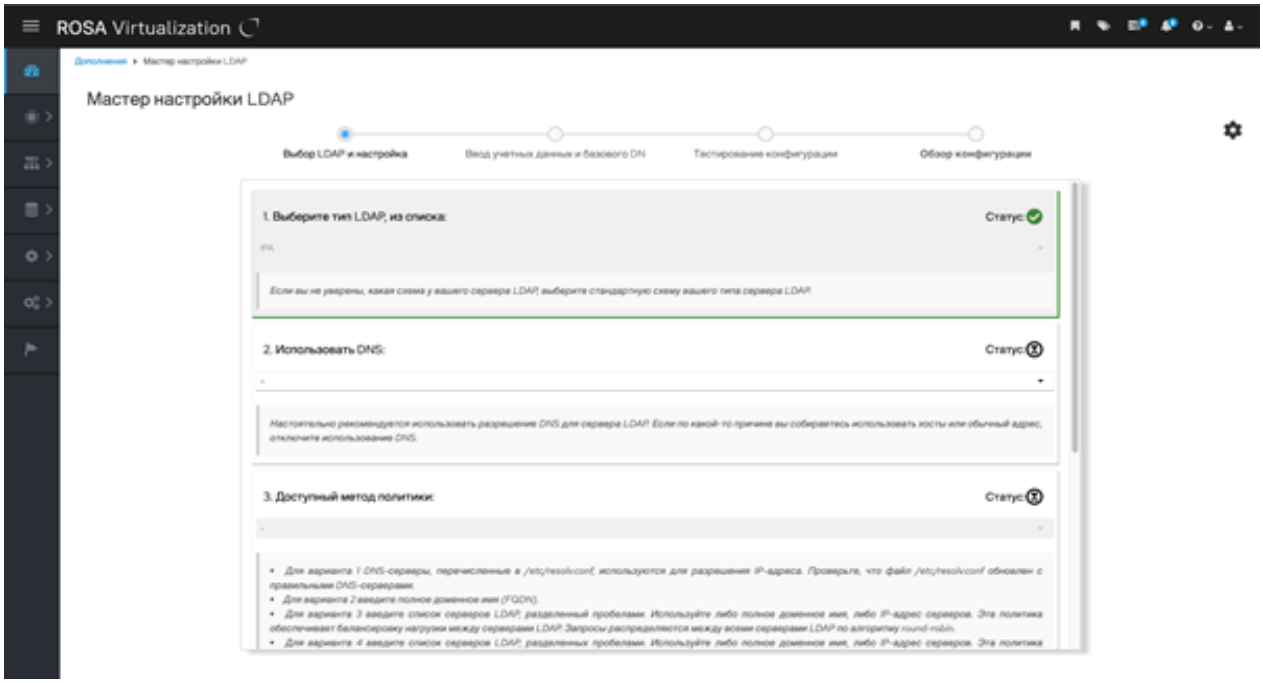

Рисунок 101 – Выбор типа LDAP сервера, использования DNS и политик использования

б) нажать кнопку Далее для перехода на следующий экран "Мастера настройки LDAP";

в) ввести учетные данные для доступа к серверу, включающие имя пользователя и пароль, которые будут использоваться для аутентификации , а также базовый DN (Distinguished Name) — это точка, от которой будут начинаться поисковые запросы в иерархии каталога LDAP (рисунок 102);

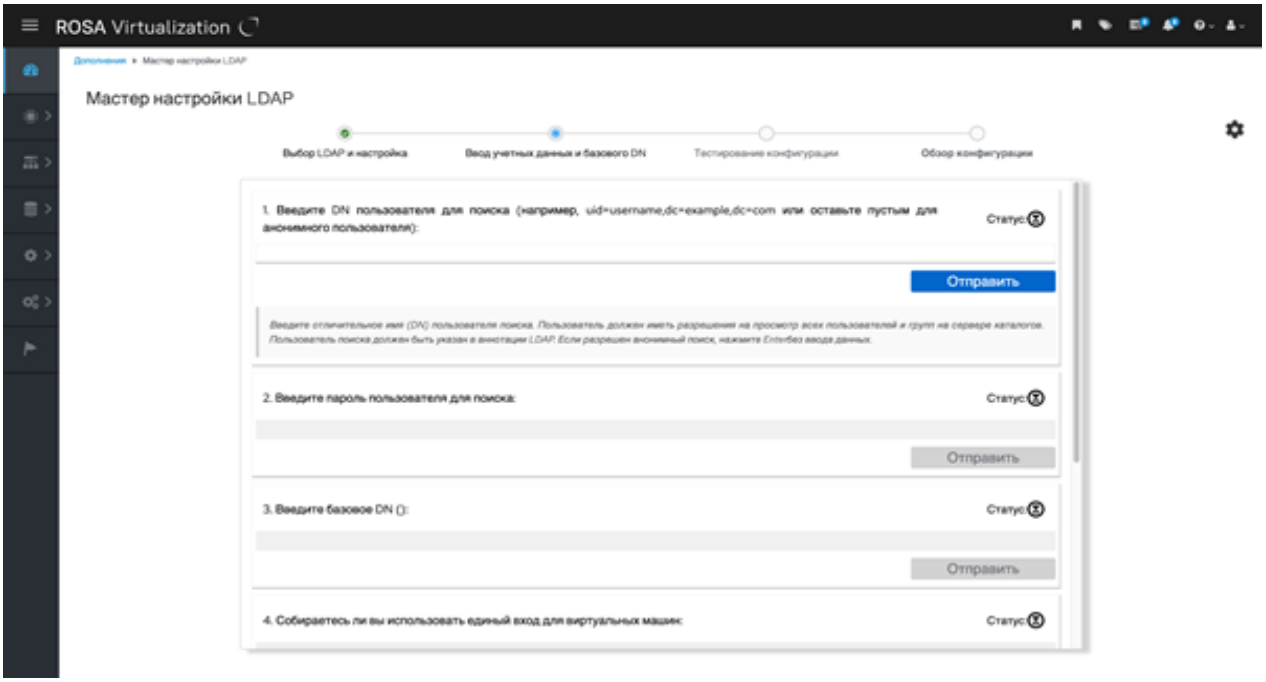

Рисунок 102 – Форма "Ввод учетных данных и базового DN" Мастера настройки LDAP

г) нажать на кнопку Далее для перехода в форму "Тестирование конфигурации";

д) протестировать введенные параметры, чтобы убедиться, что Система может успешно подключиться к LDAP-серверу и выполнить необходимые запросы (рисунок 103). Тестирование включает проверку корректности подключения, аутентификации пользователя, а также доступности и правильности структуры данных, связанных с введенным базовым DN. Если тестирование выявило ошибки, необходимо прервать процесс и начать настройку сначала.

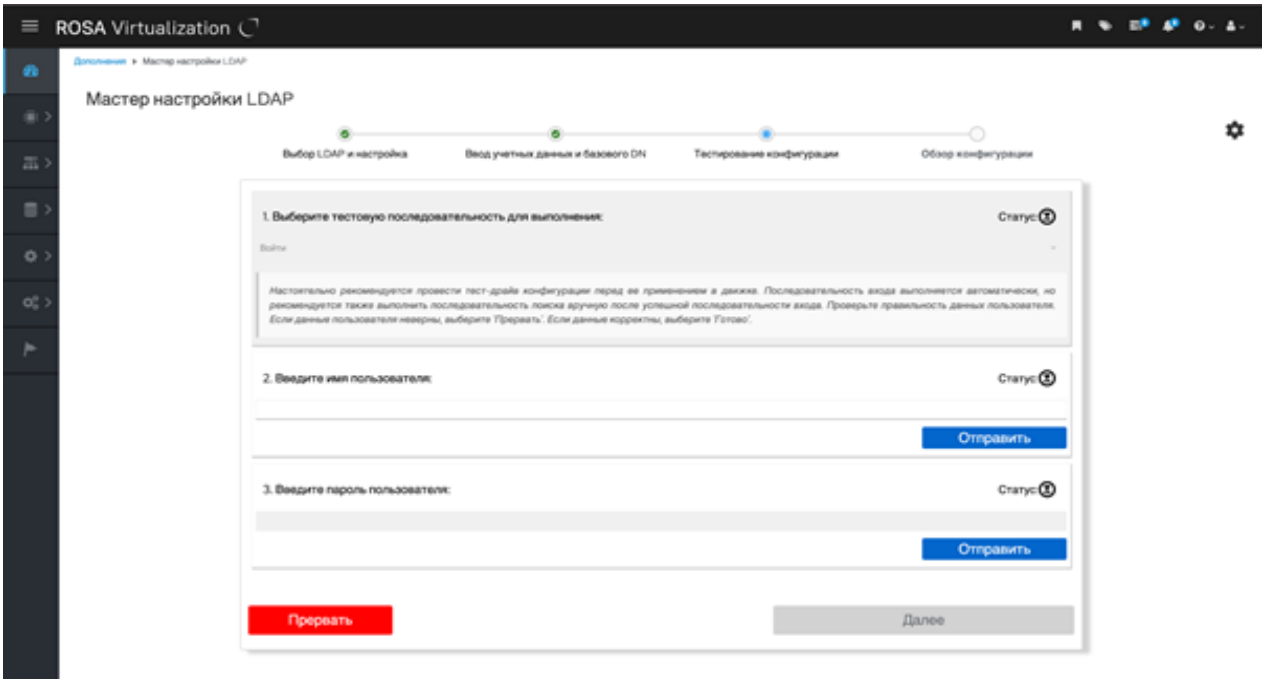

Рисунок 103 – Тестирование конфигурации LDAP

е) на последнем экране "Мастера настройки LDAP" отображается настроенная конфигурация, которую проанализировать и убедиться, что все настройки введены корректно и соответствуют требованиям; нажать на кнопку Завершить для завершения настройки конфигурации LDAP (рисунок 104).

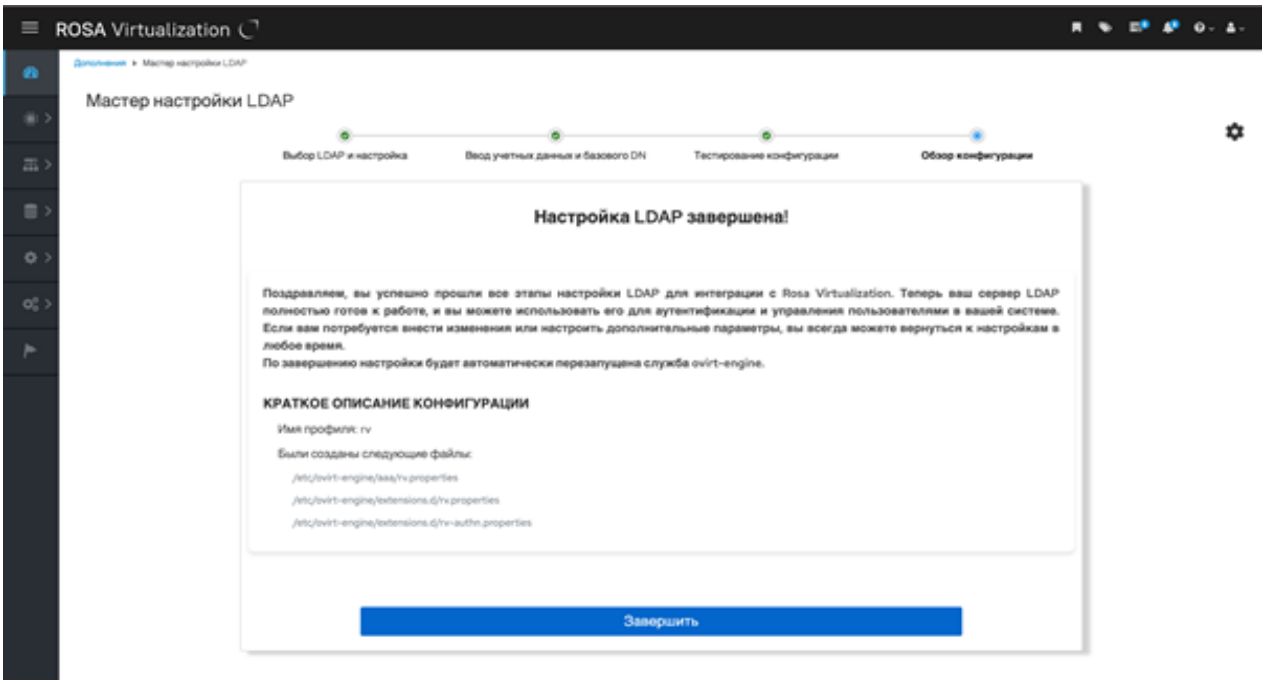

Рисунок 104 – Обзор конфигурации настройки интеграции с LDAP сервером

По завершении настройки будет автоматически перезапущена служба ovirt-engine.

3.9.2.1 Удаление LDAP-сервера

Для удаления LDAP-сервера нужно нажать на кнопку Удалить LDAP-сервер в правой верхней части окна (рисунок 105).

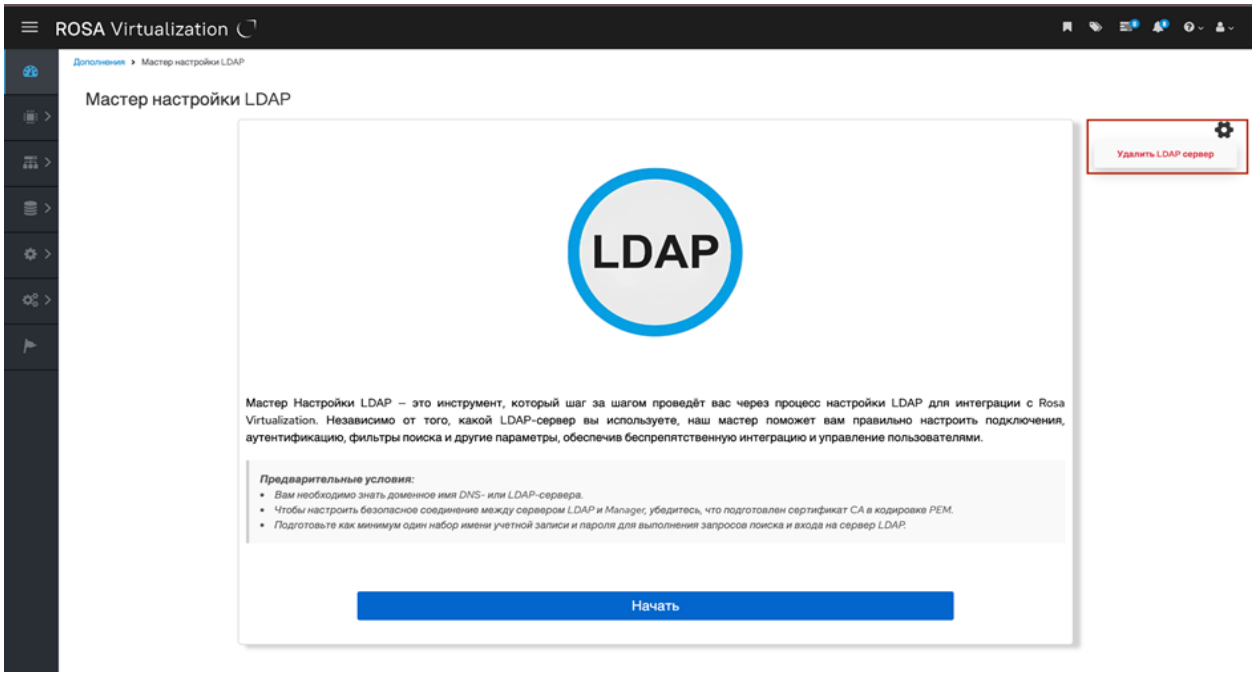

Рисунок 105 – Удаление LDAP-сервера

В появившемся диалоговом окне нужно выбрать нужный профиль из выпадающего списка, который отображает все доступные LDAP-профили и подтвердить удаление нажатием кнопки Удалить (рисунок 106). Будет отображен статус, подтверждающий успешное удаление профиля или указывающий на возможные ошибки, которые требуют внимания.

Важно – Следует убедиться, что выбран верный профиль, так как это действие нельзя будет отменить

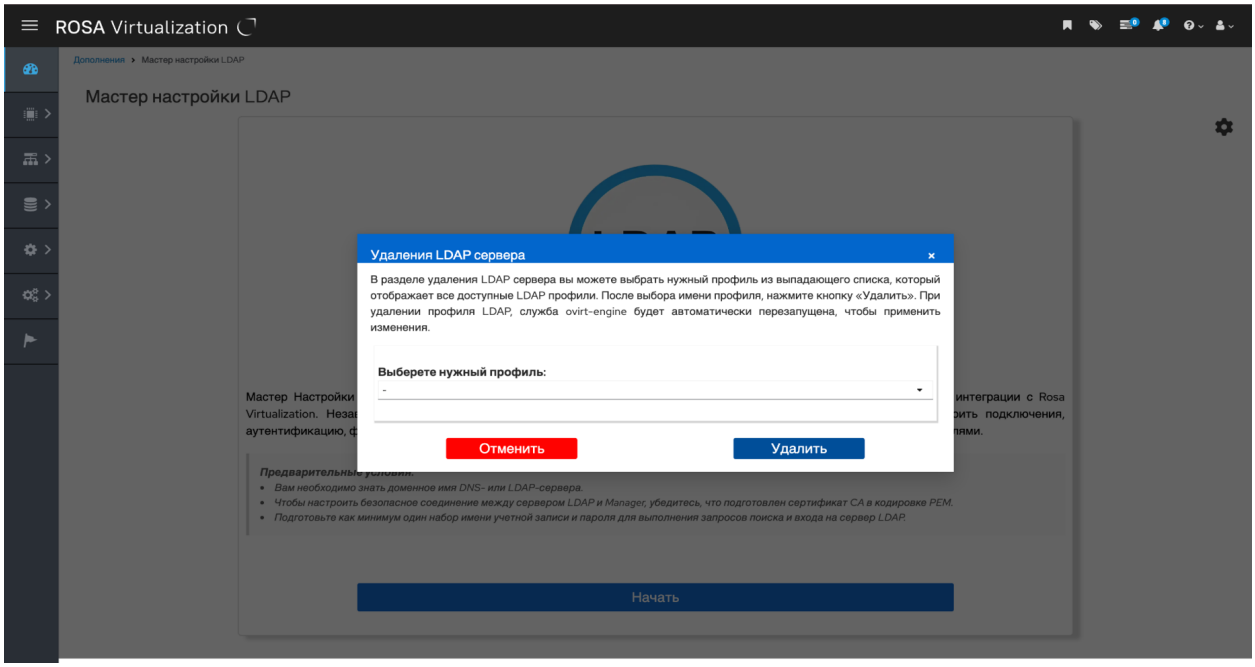

Рисунок 106 – Подтверждение удаления

По завершении удаления профиля LDAP служба ovirt-engine будет автоматически перезапущена, чтобы применить изменения в Системе. Этот шаг гарантирует, что все изменения, связанные с удалением профиля LDAP, будут правильно интегрированы в Систему.

После перезапуска службы рекомендуется проверить Систему, чтобы убедиться, что удаление прошло успешно и что все связанные процессы работают корректно.

При необходимости всегда можно повторно настроить новый LDAP-профиль или внести изменения в текущую конфигурацию.

3.9.3 Создание профиля подключения к службе каталогов LDAP сервера IPA с помощью командной строки

Настройка подключения РОСА Виртуализация к службе каталогов LDAP сервера IPA с помощью командной строки осуществляется утилитой ovirt-engine-extension-aaa-ldap-setup в консоли СУСВ.

Примечание – Если ранее уже была настроена интеграция с LDAP-сервером с помощью веб-интерфейса и "Мастера настройки LDAP", то данный пункт можно пропустить.

Для подключения к консоли СУСВ по SSH нужно выполнить 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 РОСА Виртуализация к службе каталогов LDAP

Для запуска интерактивного сценария настройки и создания профиля подключения с целью идентификации и аутентификации доменных пользователей нужно выполнить 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** следует ввести 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, нажать клавишу `Enter` или ввести "Yes".

– При отсутствии в сети сервера DNS ввести "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 РОСА Виртуализация и СУСВ. Следует отредактировать файл /etc/hosts на каждом из перечисленных выше хостов и серверов, указав актуальные доменные имена и IP-адреса.

Из пронумерованного списка нужно выбрать метод реализации политики службы DNS. При выборе варианта 1 (Single server) ввести 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 актуальном 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. В ответ на запросы сценария необходимо ввести 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 следует использовать отличительное имя служебной учетной записи, созданной ранее на сервере IPA для выполнения синхронизации с РОСА Виртуализация.

Для проверки корректности указанного отличительного имени dn используют на сервере IPA 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, нужно нажать клавишу `Enter`.

Сценарий настройки предложит указать имя для профиля подключения. В ответ на запрос сценария следует ввести 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 РОСА Виртуализация (рисунок 107).

Для тестовой проверки подключения следует указать 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 необходимо выполнить 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 107) или на Портал ВМ.

3.9.4 Вход в Портал администрирования и Портал ВМ с использованием логина и пароля корпоративного LDAP-сервера

Для входа необходимо открыть в новом окне браузера форму входа на Портал администрирования или Портал виртуальных машин и выбрать Портал администрирования (для учетной записи администратора) или Портал виртуальных машин (для учетной записи пользователя).

Затем в выпадающем меню "Профиль" следует выбрать домен авторизации, настроенный при конфигурировании доступа к серверу LDAP. В полях "Имя пользователя" и "Пароль" нужно указать логин и пароль учетной записи пользователя, настроенной в корпоративном LDAP-сервере (контроллере домена). Далее нужно нажать на кнопку `Вход в систему` (рисунок 107). При наличии у пользователя соответствующих прав будет осуществлен вход в Портал.

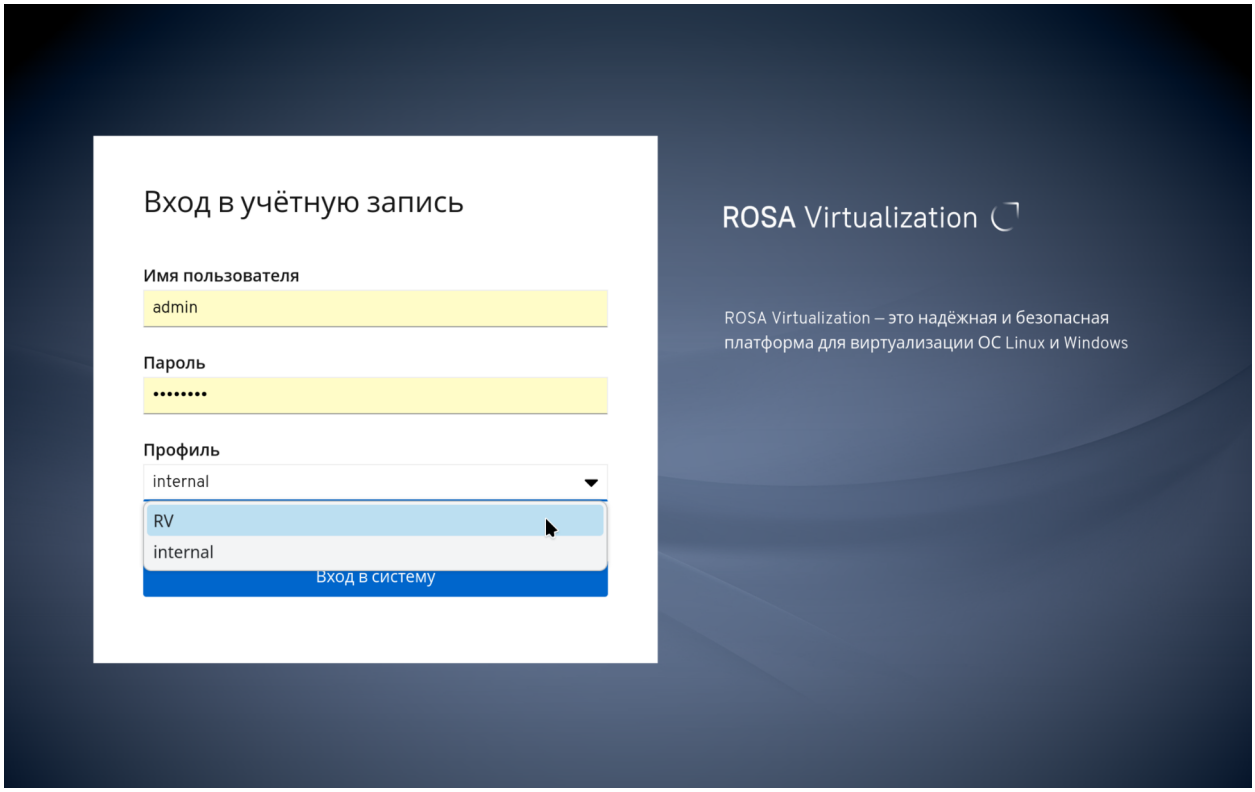

Рисунок 107 – Выбор профиля подключения в окне авторизации при входе на Портал администрирования СУСВ

3.9.4.1 Предоставление прав доступа к ресурсам РОСА Виртуализация для пользователей сервера IPA

Назначение необходимых прав доступа к ресурсам РОСА Виртуализация для новых созданных пользователей сервера IPA осуществляется на Портале администрирования СУСВ выполнением следующих действий:

а) для доступа к списку пользователей выбрать пункт "Администрирование → Пользователи" в главном меню СУСВ (рисунок 108).

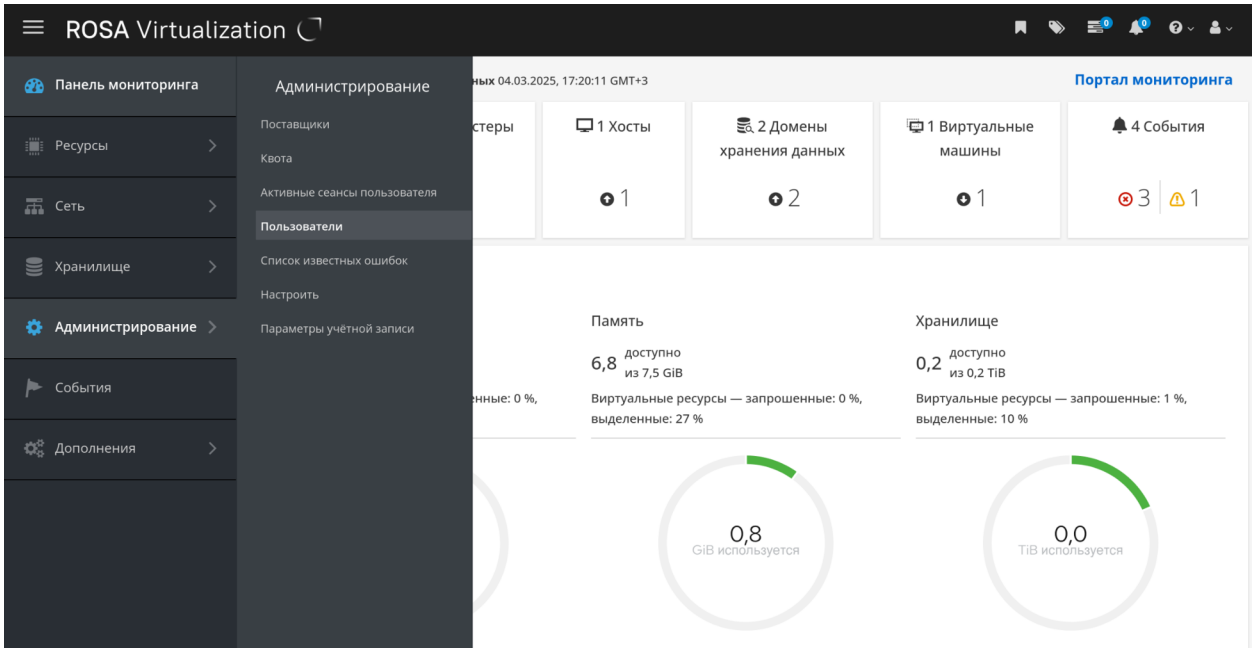

Рисунок 108 – Раздел в главном меню панели администрирования СУСВ

На странице "Администрирование → Пользователи" отображается список пользователей, авторизованных для работы с РОСА Виртуализация (рисунок 109).

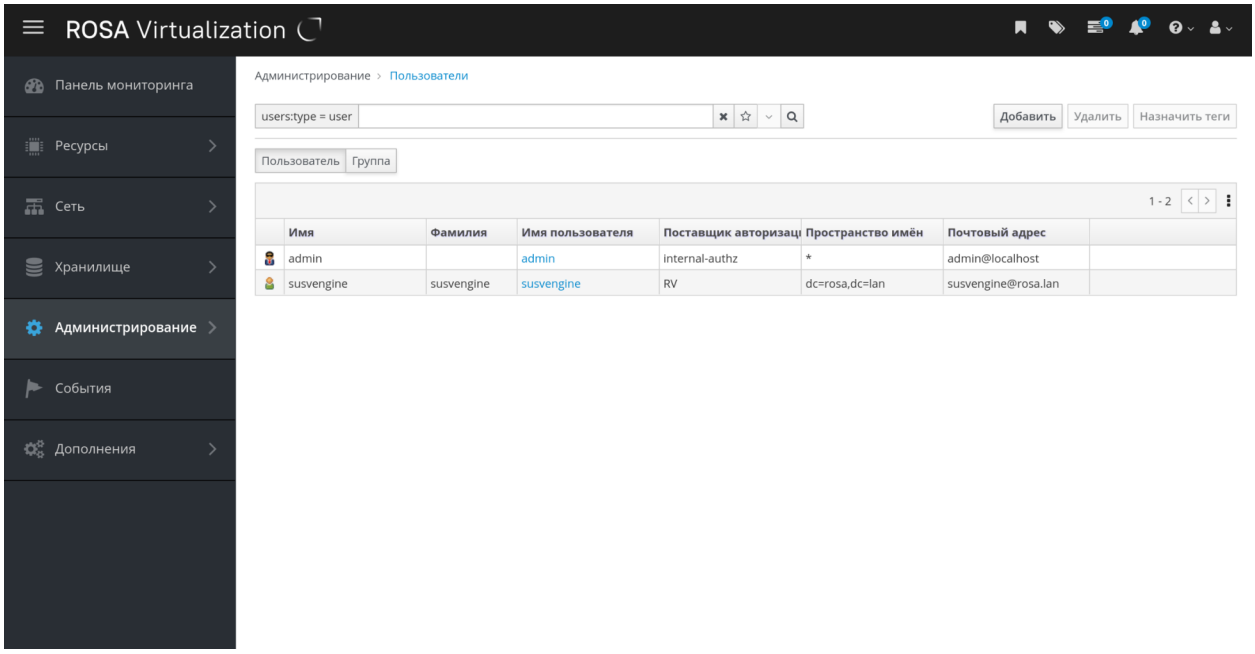

Рисунок 109 – Список пользователей, авторизованных для работы с РОСА Виртуализация

б) для добавления пользователя нажать на кнопку Добавить;

в) ввести в форму логин пользователя, принадлежащего пространству имён присоединенного домена, и нажать на кнопку Вперед (рисунок 110);

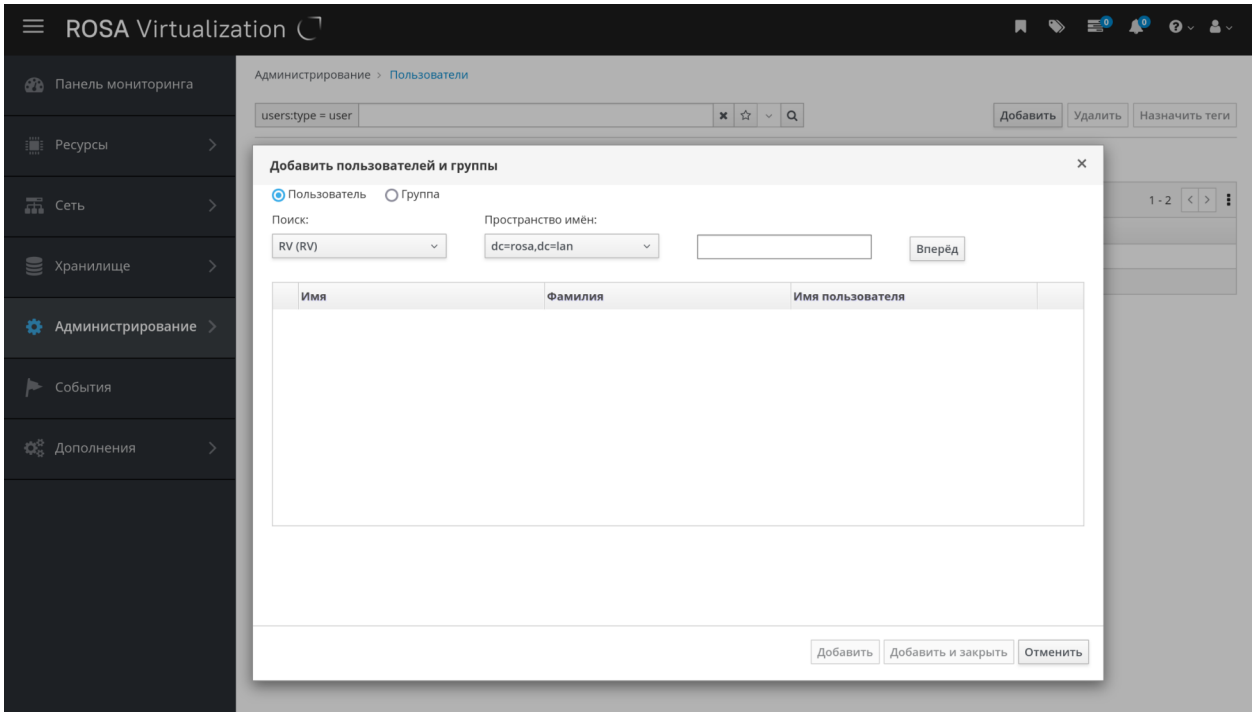

Рисунок 110 – Добавление пользователя из корпоративного каталога LDAP

г) выбрать необходимого пользователя и нажать на кнопку Добавить и закрыть (рисунок 111).

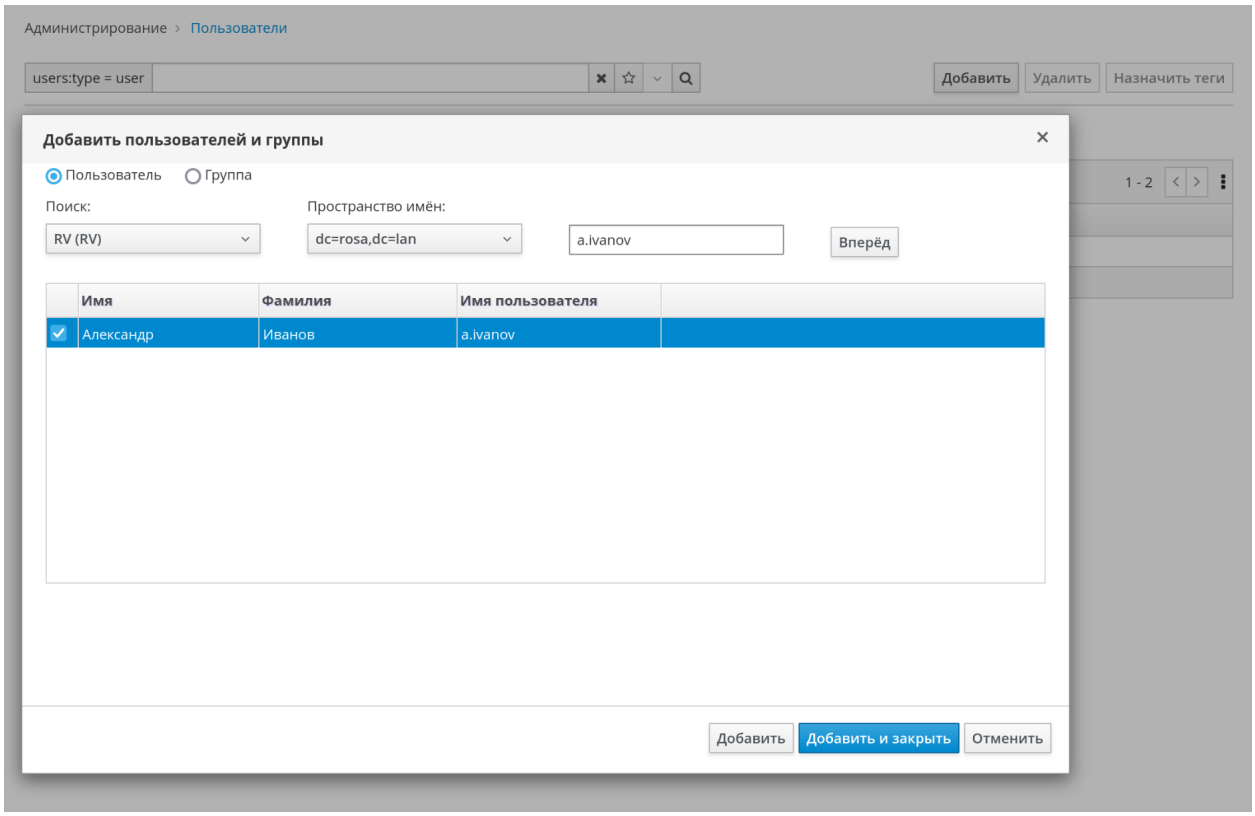

Рисунок 111 – Поиск пользователя домена по логину

Пользователь будет добавлен к списку пользователей, авторизованных для работы с РОСА Виртуализация (рисунок 112).

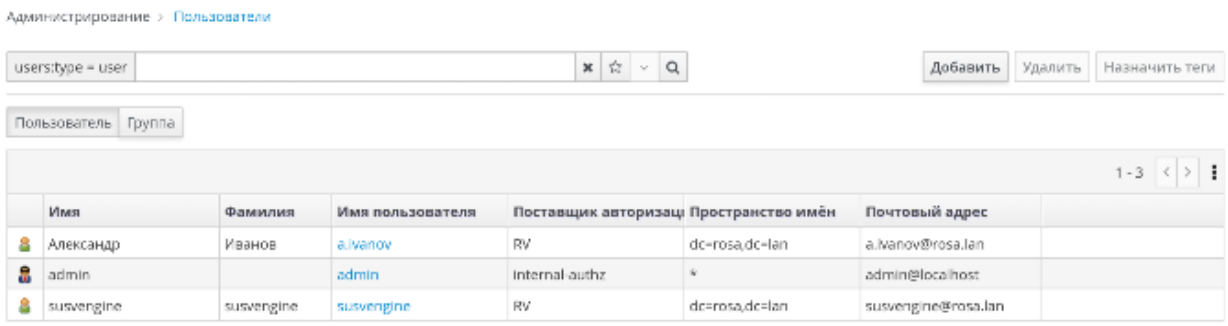

Рисунок 112 – Обновленный список пользователей средства виртуализации

Далее необходимо предоставить пользователю права на доступ к конкретным ресурсам с помощью следующих шагов:

а) нажать на логин пользователя в списке (рисунок 112). Откроется форма с информацией о данном пользователе (рисунок 113);

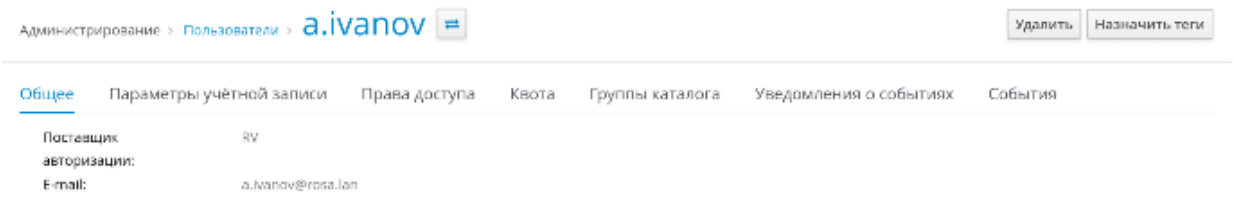

Рисунок 113 – Информация о пользователе a.ivanov

б) перейти на вкладку "Права доступа";

в) нажать на кнопку Добавить системные полномочия (рисунок 114);

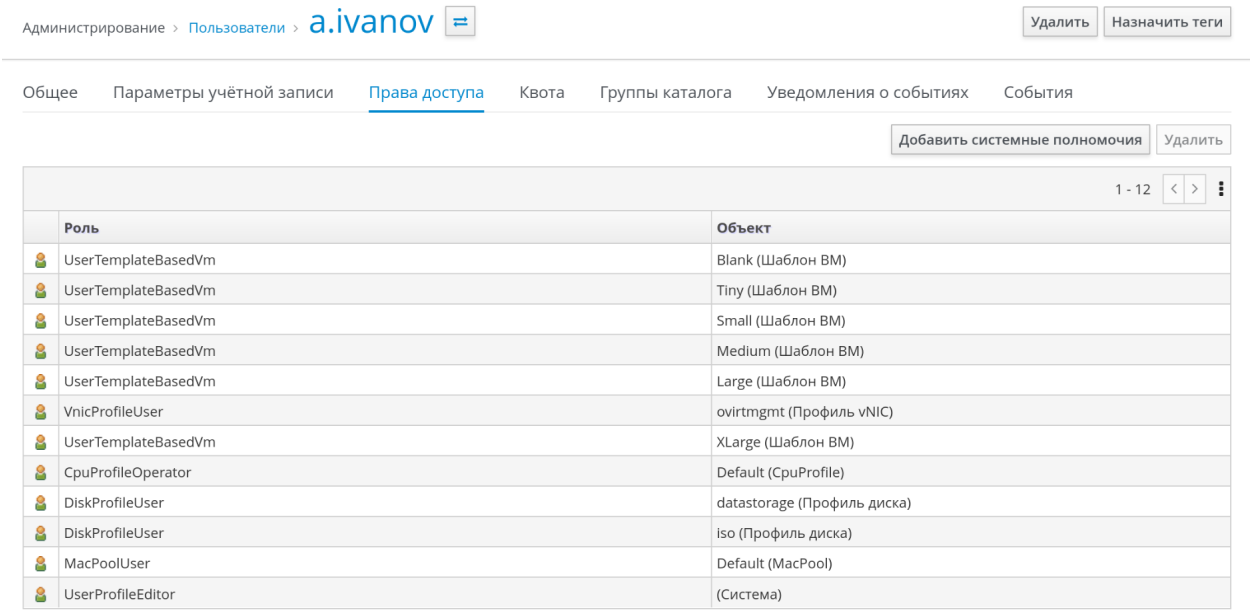

Рисунок 114 – Права доступа пользователя

г) выбрать требуемые полномочия во вкладке "Права доступа" по кнопке Добавить системные полномочия Например, для опытного пользователя можно выбрать PowerUserRole (пользователь с расширенными полномочиями) (рисунок 115).

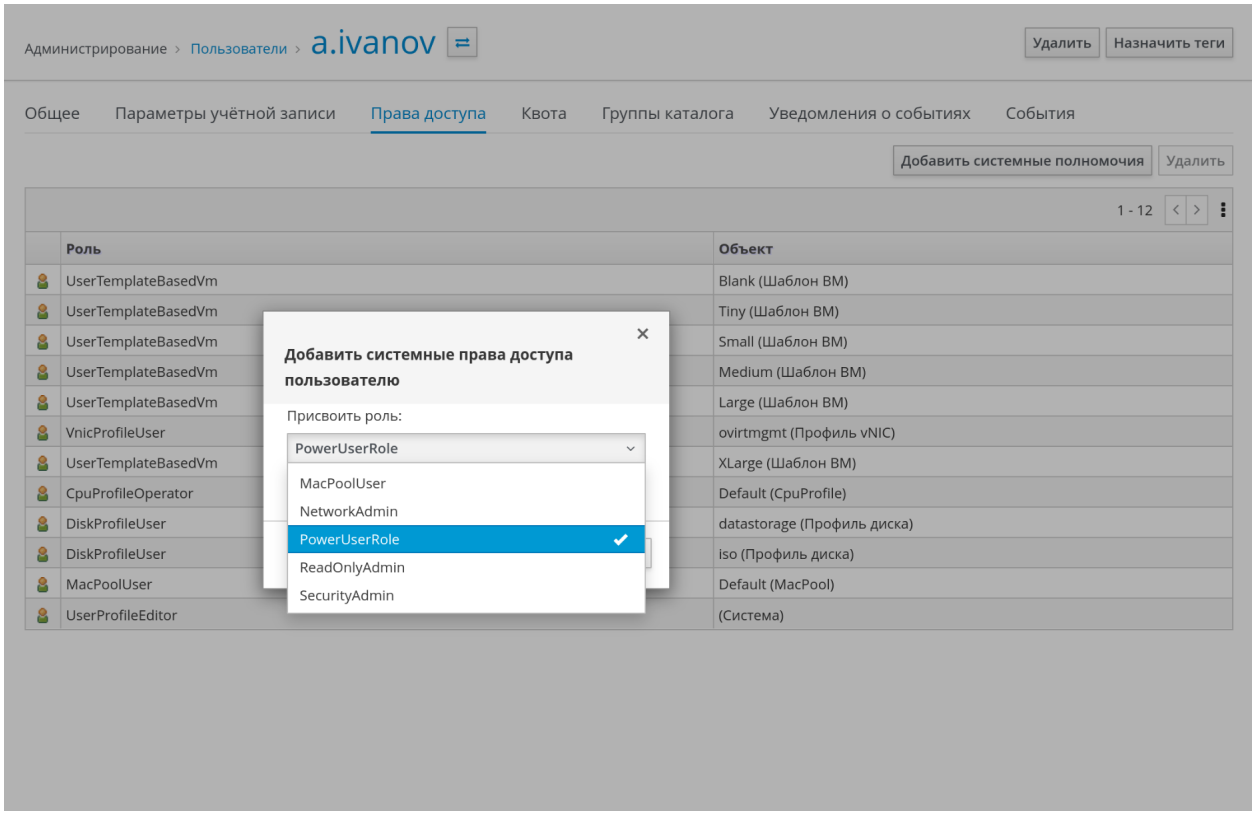

Рисунок 115 – Добавление системных полномочий

д) после выбора необходимых прав нажать на кнопку `OK` для добавления указанных прав и полномочий (рисунок 116).

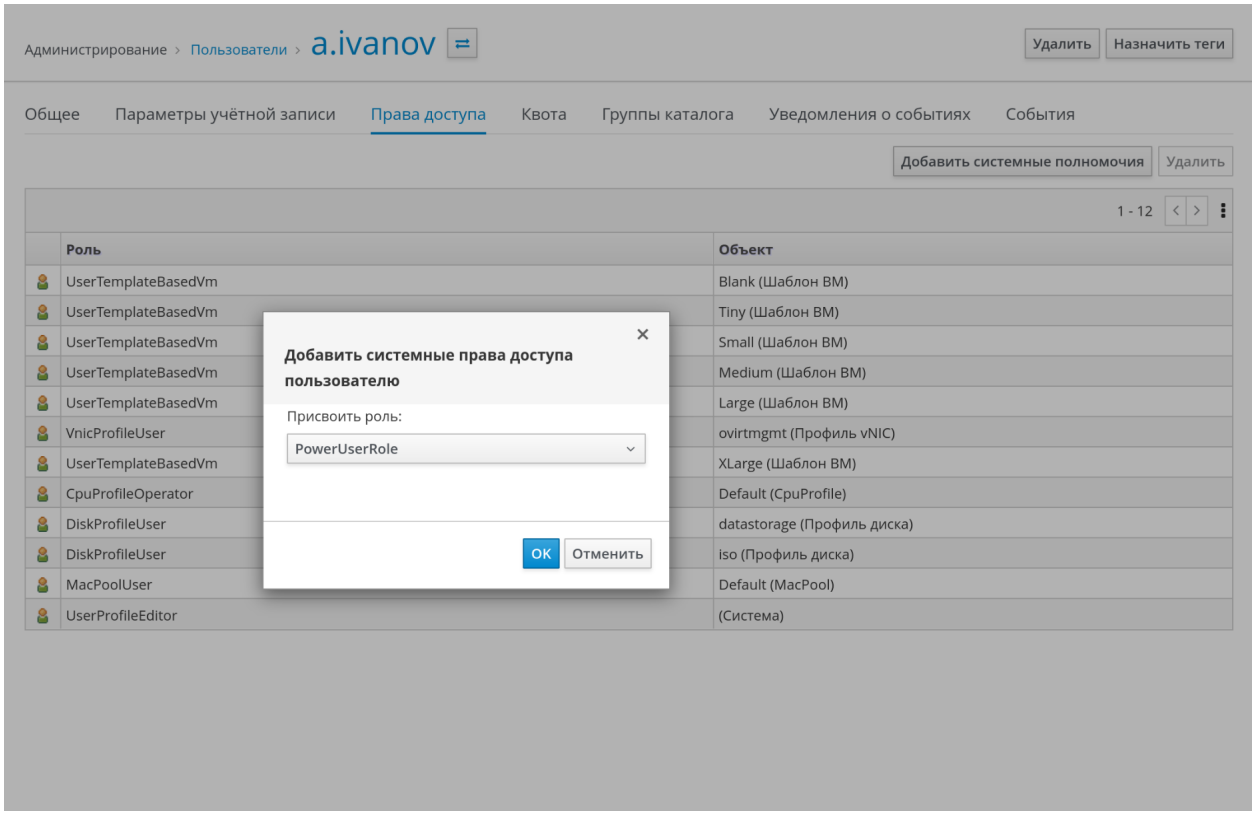

Рисунок 116 – Добавление выбранных прав пользователю

Выбранные права появятся в списке прав пользователя (рисунок 117).

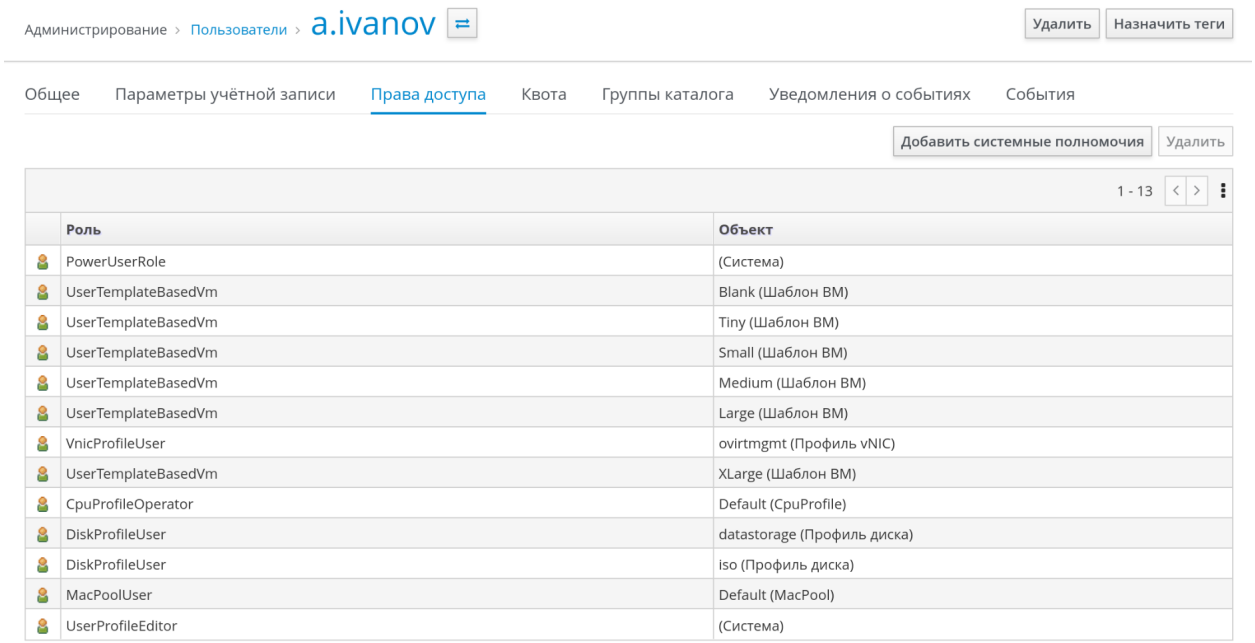

Рисунок 117 – Обновленный список прав пользователя

Для проверки выбранных прав нужно войти 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 118).

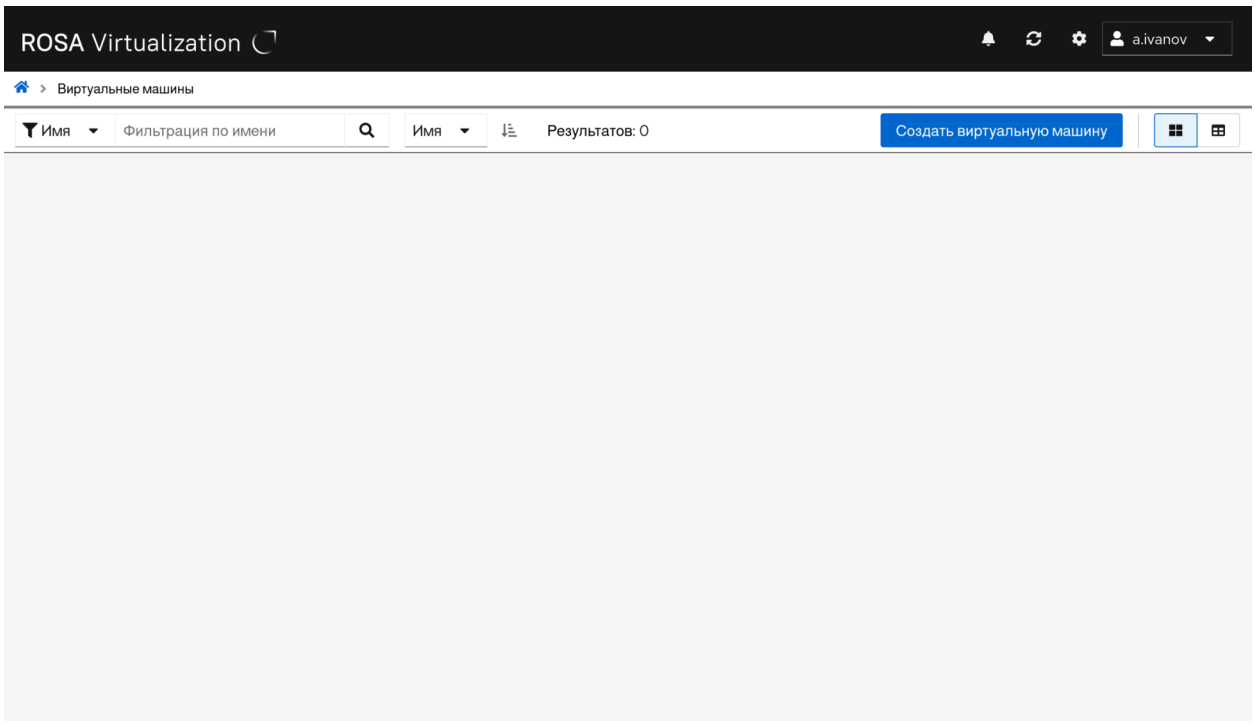

Рисунок 118 – Интерфейс Портала ВМ, доступный пользователю с правами PowerUserRole

Для создания ВМ можно нажать на кнопку `Создать виртуальную машину` (рисунок 118).

В результате откроется интерфейс для создания ВМ (доступно пользователю с ролью PowerUserRole) (рисунок 119).

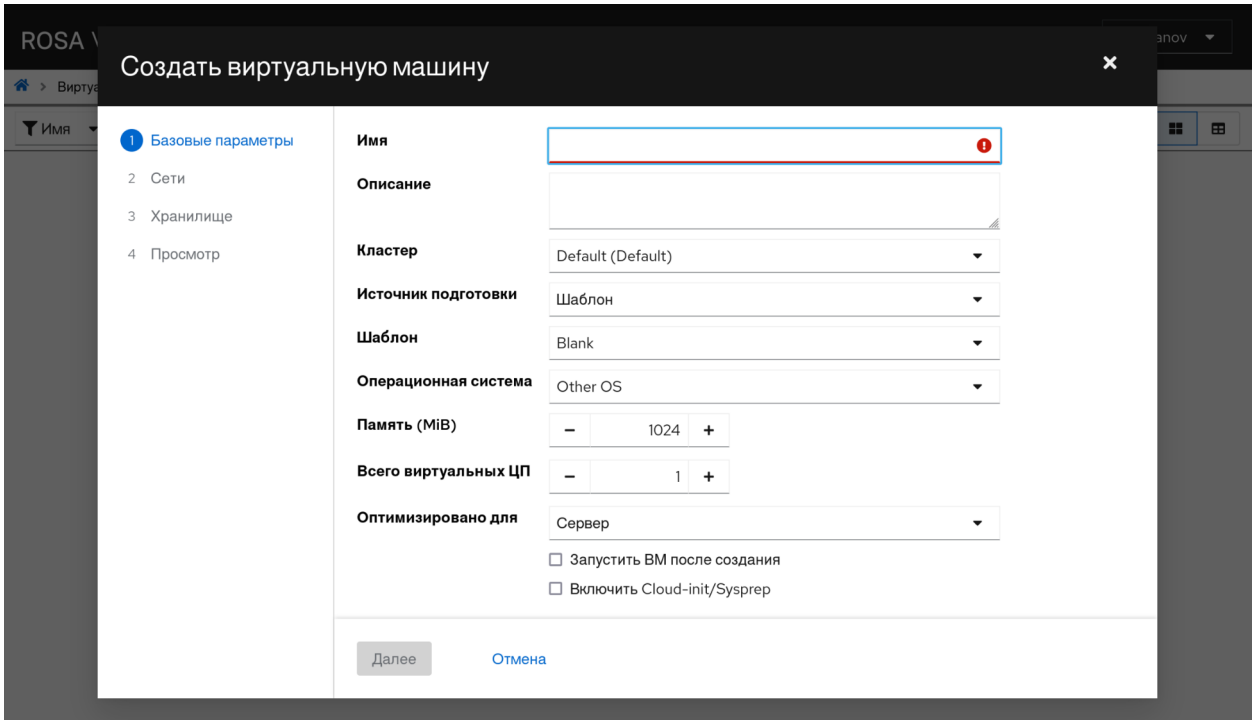

Рисунок 119 – Интерфейс создания ВМ для пользователя с ролью PowerUserRole

При необходимости можно повторить операцию по добавлению пользователей и наделению их правами для других пользователей, зарегистрированных на корпоративном LDAP-сервере.

4 РАЗВЕРТЫВАНИЕ ВНЕШНЕГО KEYCLOAK И ИНТЕГРАЦИЯ С СУСВ

В составе РОСА Виртуализация сервис Keycloak используется в качестве инструмента для управления идентификацией и доступом, который предоставляет функции единого входа (SSO) и предназначен для идентификации и аутентификации пользователей.

4.1 Развертывание внешнего Keycloak

Сервис Keycloak может быть развернут как на отдельном физическом сервере, так и на ВМ, находящейся вне кластера управляемого СУСВ (oVirt).

Рекомендованная к использованию версия Keycloak — 15 и выше.

Сервер должен соответствовать следующим требованиям:

– процессор: архитектура x86_64;
– количество ядер: не менее 2;
– оперативная память: не менее 4 ГБ;
– свободное дисковое пространство: не менее 40 ГБ;
– сетевой интерфейс: не менее 1 Гбит/с;
– Сеть: доступ из oVirt Engine по HTTPS (порт 8443 или 443);
– ОС: CentOS Stream 8 / Rocky Linux 8;
– привод DVD / порт USB – для установки ПО.

Приведенные далее рекомендации основаны на версии Keycloak 15.1.1 и ОС CentOS Stream 8. Настройки на других версиях могут иметь некоторые отличия. Для уточнения необходимо обращаться к документации по применяемым программным продуктам.

4.1.1 Подготовка окружения

Необходимо выполнить следующие подготовительные действия:

а) создать пользователя и группы:

```
sudo groupadd -r keycloak
sudo useradd -m -d /var/lib/keycloak -s /sbin/nologin \
-r -g keycloak keycloak
```

б) создать каталог под Keycloak:

```
sudo mkdir -p /opt/keycloak
```

в) загрузить дистрибутив Keycloak:

```
sudo wget https://github.com/keycloak/keycloak/releases/ \
download/15.1.1/keycloak-15.1.1.zip -P /opt/keycloak
```

г) распаковать дистрибутив Keycloak:

```
sudo unzip /opt/keycloak/keycloak-15.1.1.zip -d \
/opt/keycloak
cd /opt
```

д) назначить права пользователю Keycloak:

```
sudo chown -R keycloak:keycloak keycloak
sudo chmod o+x /opt/keycloak/keycloak-15.1.1/bin/
```

4.1.2 Установка и настройка дополнительного ПО

Для обеспечения работы Keycloak требуется установить Java и внешнюю базу данных PostgreSQL. Далее описаны необходимые действия по установке ПО и настройке дополнительных зависимостей:

а) Установить OpenJDK 11. Keycloak 15.x работает только на Java 8 или Java 11. Для CentOS 8 рекомендуется использовать OpenJDK 11.

Репозитории на зеркалах CentOS отключены, поэтому необходимо подключиться к доступному репозиторию:

```
# sed -i 's/mirrorlist/#mirrorlist/g' \
/etc/yum.repos.d/CentOS-*
# sed -i 's|#baseurl=http://mirror.centos.org|\
baseurl=http://vault.centos.org|g' /etc/yum.repos.d/CentOS-*
```

Установить Java:

```
sudo dnf -y install java-11-openjdk
```

Проверить версию:

```
java -version
openjdk version "11.x.x"
```

б) Установить PostgreSQL 14. Keycloak поддерживает PostgreSQL 10+, но оптимально использовать PostgreSQL 14 (стабильный и совместимый пакет для CentOS 8).

1) подключить официальный репозиторий PostgreSQL:

```
sudo dnf install -y \
https://download.postgresql.org/pub/repos/yum/reporpms/\
EL-8-x86_64/pgdg-redhat-repo-latest.noarch.rpm
```

2) отключить встроенный модуль PostgreSQL:

```
sudo dnf -qy module disable postgresql
```

3) установить сервер и клиент PostgreSQL 14:

```
sudo dnf -y install postgresql14-server postgresql14
```

4) инициализировать кластер базы данных:

```
sudo /usr/pgsql-14/bin/postgresql-14-setup initdb
```

5) добавить в автозагрузку и запустить сервис:

```
sudo systemctl enable postgresql-14
sudo systemctl start postgresql-14
```

6) проверить состояние сервиса:

```
systemctl status postgresql-14
```

Примечание – Создавать базу данных и пользователя вручную НЕ требуется. Keycloak создаст их автоматически при первом запуске — при условии, что параметры подключения корректно указаны в конфигурационном файле (рассмотрены далее).

в) Настроить SSL для Keycloak.

Keycloak должен работать по протоколу HTTPS, иначе oVirt Engine не примет соединение. Можно использовать:

– готовый сертификат (рекомендовано);
– самоподписанный (для тестовой среды).

1) создать каталог SSL (если его нет):

```
sudo mkdir -p  \
/opt/keycloak/keycloak-15.1.1/standalone/configuration/ssl
```

2) перейти в каталог SSL:

```
cd /opt/keycloak/keycloak-15.1.1/standalone/configuration/ssl
```

3) для тестовой среды можно создать самоподписанный сертификат и приватный ключ:

```
sudo openssl req -x509 -sha256 -nodes -days 365 \
-newkey rsa:2048 \
-keyout \
```

```
/opt/keycloak/keycloak-15.1.1/standalone/configuration \
/ssl/server.key.pem \
-out \
/opt/keycloak/keycloak-15.1.1/standalone/configuration \
/ssl/server.crt.pem
```

В процессе выполнения команда запросит ввод значений:

– Common Name (CN) — необходимо ввести, должно совпадать с доменным именем Keycloak, например: keycloak.home.local;
– остальные поля можно оставить пустыми.

После выполнения будут созданы:

– server.key.pem — приватный ключ;
– server.crt.pem — самоподписанный сертификат.

4) Создать контейнер PKCS12.

```
cd /opt/keycloak/keycloak-15.1.1/ \
standalone/configuration/ssl

sudo openssl pkcs12 -export \
-in server.crt.pem \
-inkey server.key.pem \
-out server.p12 \
-name server \
-passout pass:password
```

5) Импортировать PKCS12 в Java Keystore Keycloak.

```
sudo keytool -importkeystore \
-srckeystore server.p12 -srcstoretype PKCS12 \
-srcstorepass password \
-destkeystore application.keystore -deststoretype JKS \
-deststorepass password
```

Примечание – Пароль указывается в конфигурационном файле standalone.xml.

4.1.3 Настройка Keycloak

После установки Keycloak необходимо изменить базовую конфигурацию сервера приложений WildFly, подключить базу данных и подготовить окружение для работы с oVirt:

а) В файле конфигурации standalone.xml, расположенном в папке /opt/keycloak/keycloak-15.1.1/standalone/configuration/:

1) Указать в файле пользователя и пароль для автоматического

```xml
<datasource jndi-name="java:jboss/datasources/KeycloakDS" pool-
name="KeycloakDS" enabled="true" use-java-context="true" statistics-
enabled="${wildfly.datasources.statistics-enabled:${wildfly.statistics-
enabled:false}}">
                    <connection-url>jdbc:h2:${jboss.server.data.dir}/
keycloak;AUTO_SERVER=TRUE</connection-url>
                    <driver>h2</driver>
                    <security>
                        <user-name>keycloak</user-name>
                        <password>12345</password>
                    </security>
                </datasource>
                <drivers>
                    <driver name="h2" module="com.h2database.h2">
                        <xa-datasource-class>org.h2.jdbcx.JdbcDataSource</
xa-datasource-class>
                    </driver>
                </drivers>
            </datasources>
```

Рисунок 120 –Имя пользователя и пароль для БД Keycloak

создания БД Keycloak (рисунок 120).

2) Указать доменное имя для Keycloak (рисунок 121). Для примера использовано имя keycloak.home.local. При настройке необходимо указать ваш реальный домен Keycloak. Домен должен быть прописан в DNS (или в /etc/hosts).

```xml
<spi name="hostname">
    <default-provider>default</default-provider>
    <provider name="default" enabled="true">
        <properties>
            <property name="hostname" value="keycloak.home.local"/>
            <property name="strict-https" value="true"/>
            <property name="frontend-url" value="https://
keycloak.home.local:8443/"/>
        </properties>
    </provider>
</spi>
```

Рисунок 121 –Доменное имя для Keycloak

б) Создать администратора Keycloak.

```
cd /opt/keycloak/keycloak-15.1.1/bin
sudo ./add-user-keycloak.sh -r master -u admin
```

в) Открыть порт 8443 для взаимодействия по протоколу HTTPS.

```
sudo firewall-cmd --permanent --zone=public \
--add-port=8443/tcp
sudo firewall-cmd --reload
```

г) Запустить сервис Keycloak.

```
sudo /opt/keycloak/keycloak-15.1.1/bin/standalone.sh \
-b 0.0.0.0
```

Дальнейшая настройка Keycloak проводится в веб-интерфейсе сервиса:

а) Войти в веб-интерфейс (рисунок 122), для чего:

1) в браузере перейти по адресу доменного имени Keycloak, например: https:// keycloak.home.local:8443;
2) указать Логин: admin;
3) ввести Пароль: указанный при создании администратора.

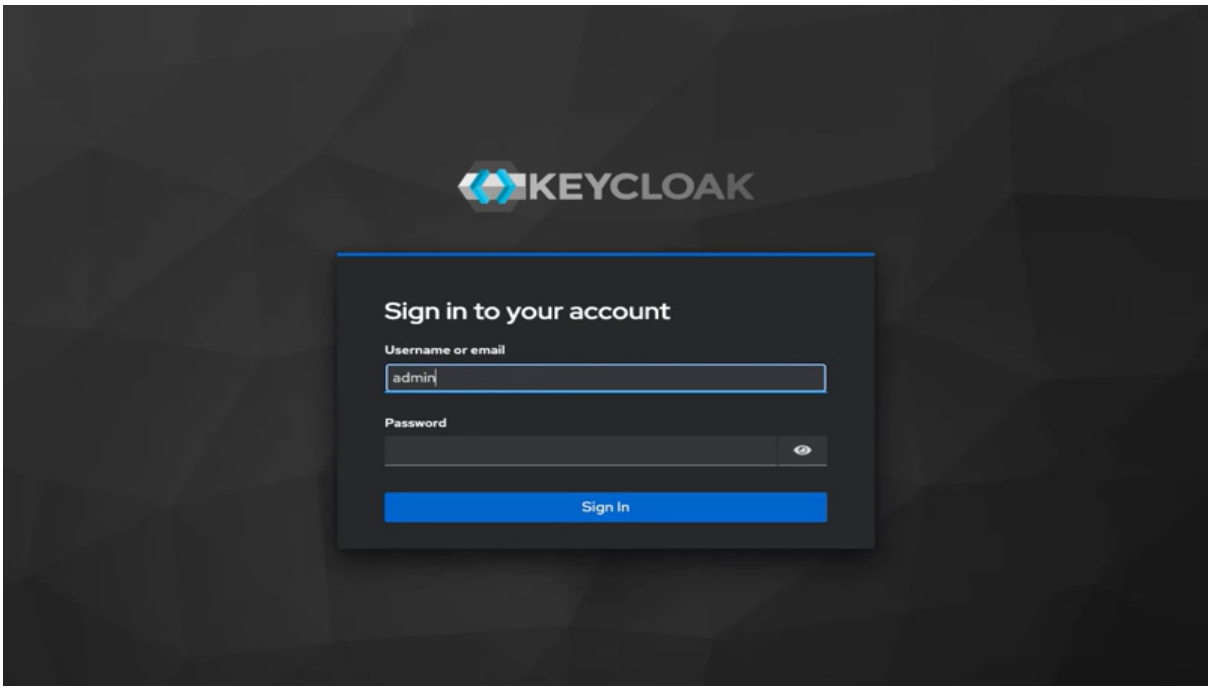

Рисунок 122 –Вход в Keycloak

б) Создать realm. В главном меню нажать `Add realm` (рисунок 123). Задать имя "ovirt-internal" для нового realm. Дальнейшая настройка будет производиться в нем (рисунок 124).

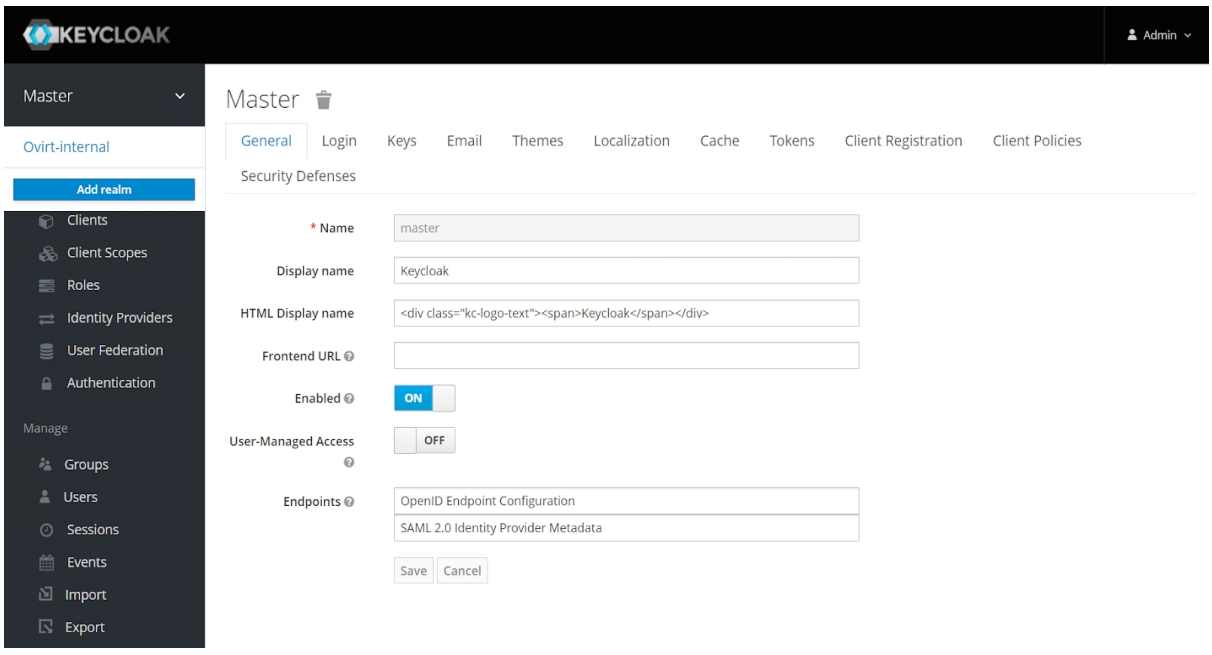

Рисунок 123 –Добавить realm

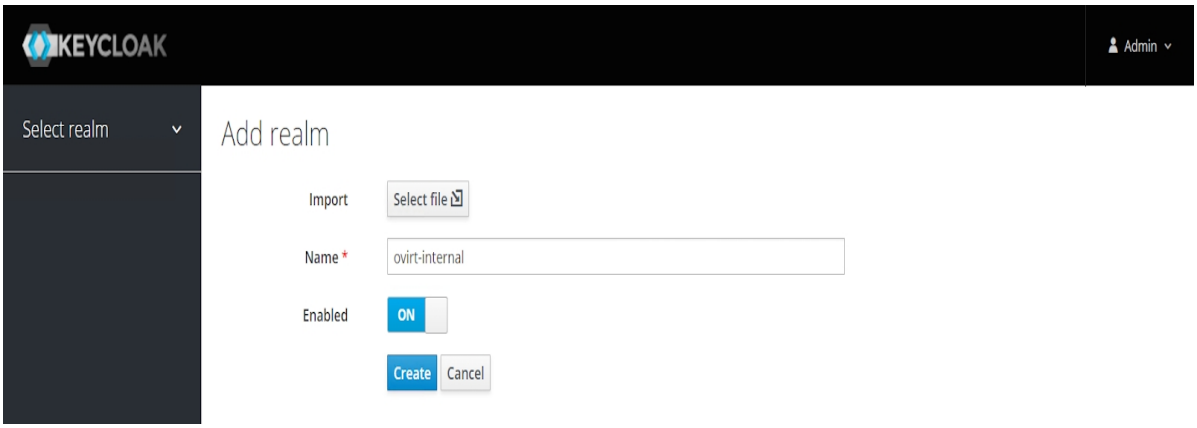

Рисунок 124 –Имя ovirt-internal для нового realm

в) Создать группу администраторов.

В разделе "Groups" нажать New, ввести имя группы ovirt-administrator (рисунок 125).

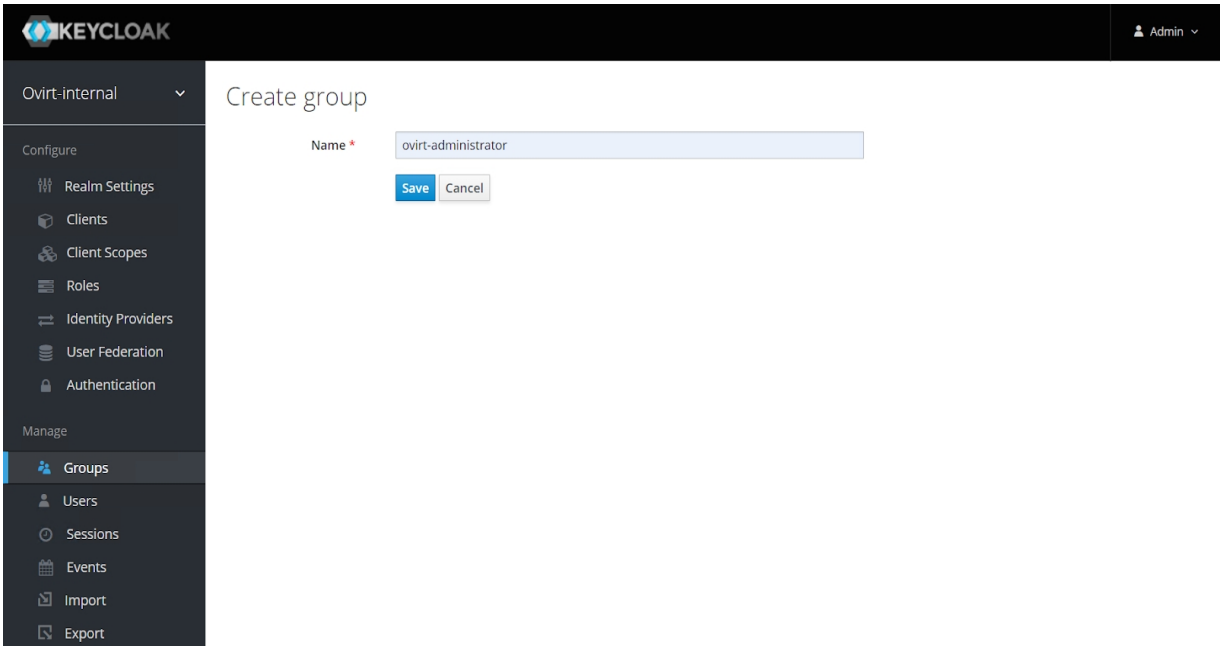

Рисунок 125 –Создать группу администраторов

г) Создать учетную запись администратора.

В разделе "Users" нажать Add user, ввести имя пользователя "admin@ovirt", Email: "admin@localhost" (важно для авторизации в Grafana), в выпадающем списке "Groups" выбрать ранее созданную группу "ovirt-administrator" (рисунок 126).

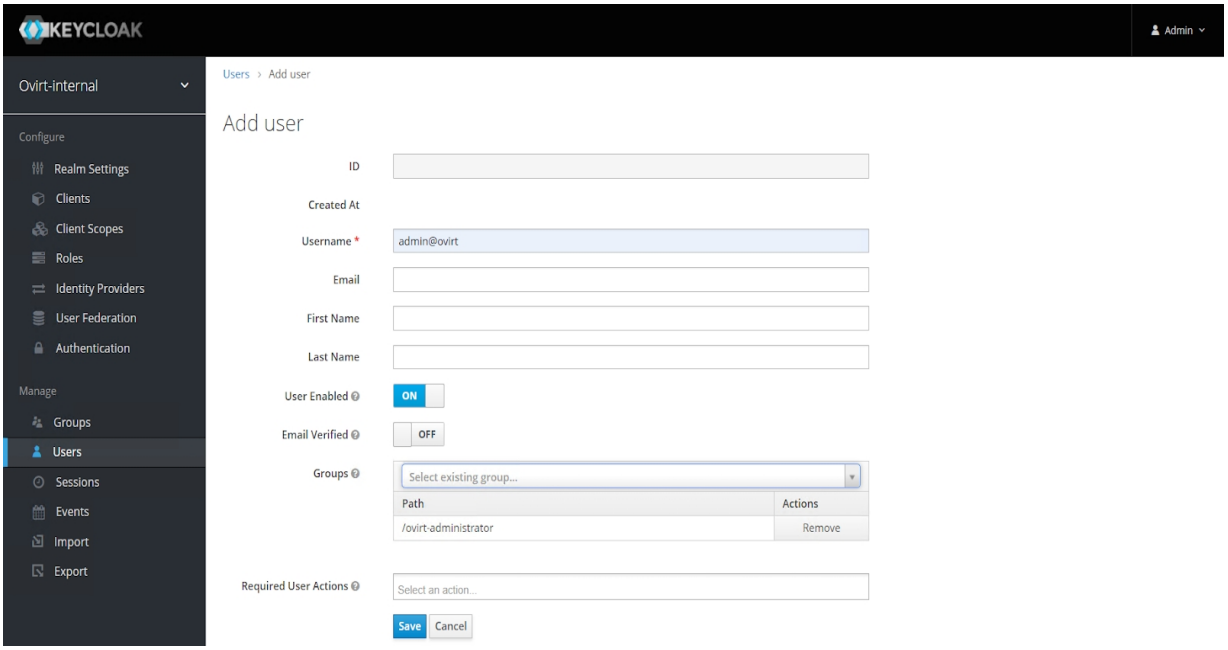

Рисунок 126 –Создать администратора

д) Настроить учетную запись администратора, выполнив необходимые действия в разделе "Users":

1) во вкладке "Users/Credentials" задать пользователю пароль нажатием кнопки `Set password`. Включенный переключатель "Temporary" указывает, что при первом входе пользователю необходимо будет ввести новый пароль (рисунок 127). Ввод подтвердить нажатием кнопки `Save`.

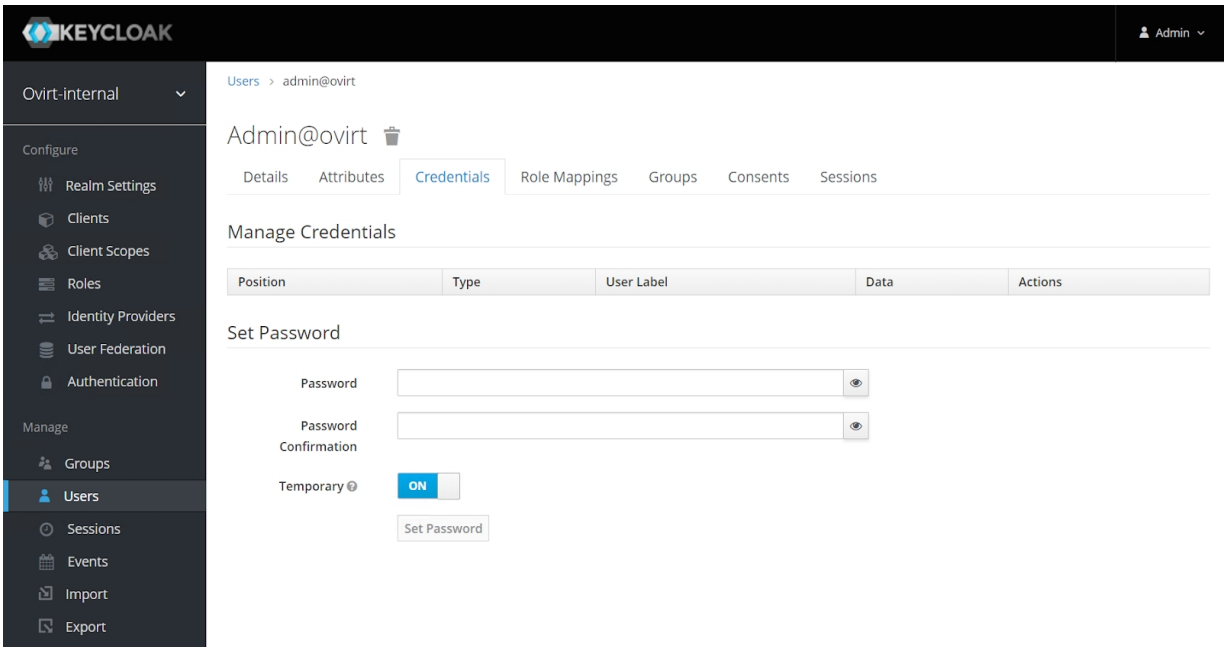

Рисунок 127 –Задать пароль администратора

2) в разделе "Roles" нажать `Add Role` (рисунок 129).

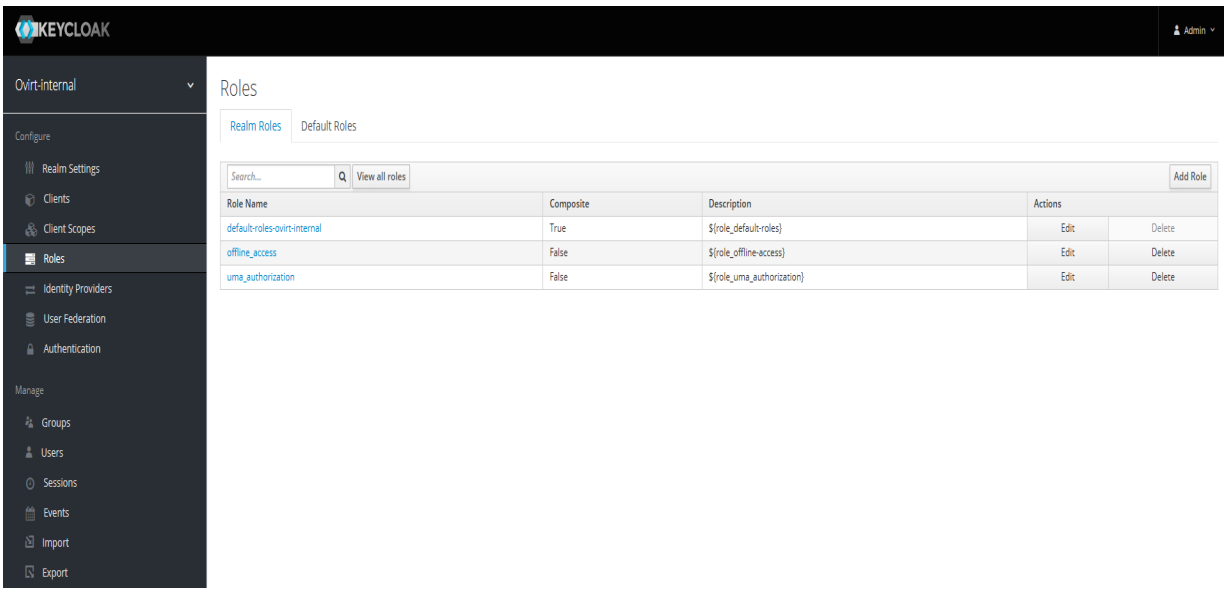

Рисунок 128 –Раздел Roles

Ввести Role Name: "grafana-admin" (рисунок 129). Ввод подтвердить нажатием кнопки `Save`.

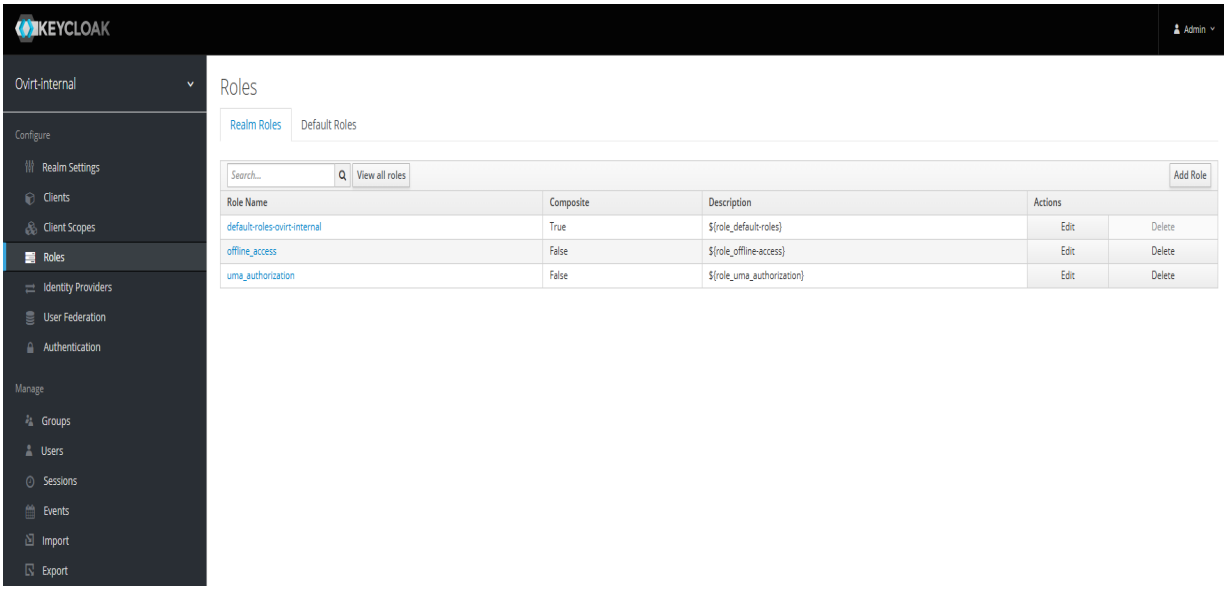

Рисунок 129 –Раздел Roles

Аналогично добавить роли grafana-editor и grafana-viewer (рисунок 130).

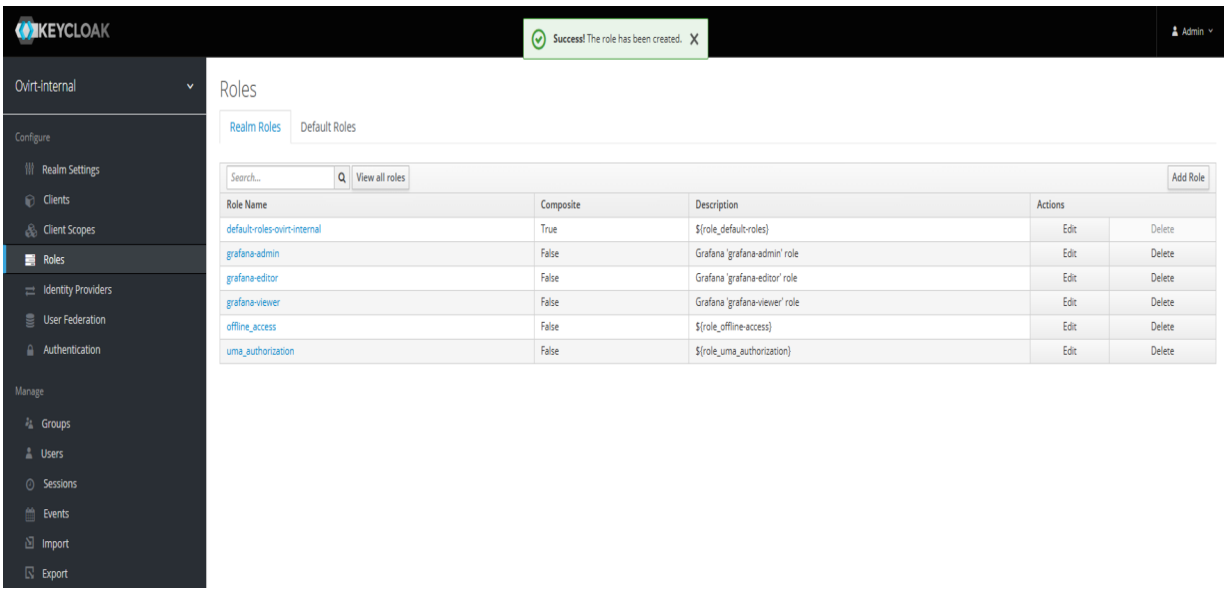

Рисунок 130 –Добавленные роли Grafana

е) Настроить Client Scopes:

1) перейти в раздел "Client Scopes" и нажать `Create` (рисунок 131).

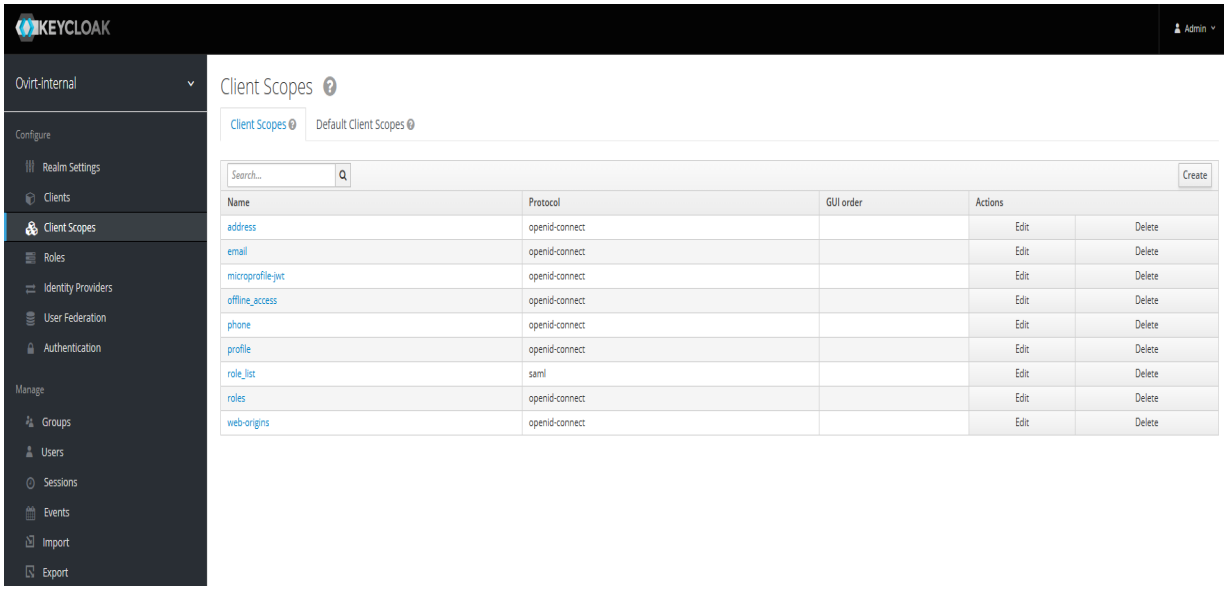

Рисунок 131 –Раздел Client Scopes

2) ввести Name: "ovirt-app-admin", остальные параметры оставить по умолчанию. Нажать Save (рисунок 132).

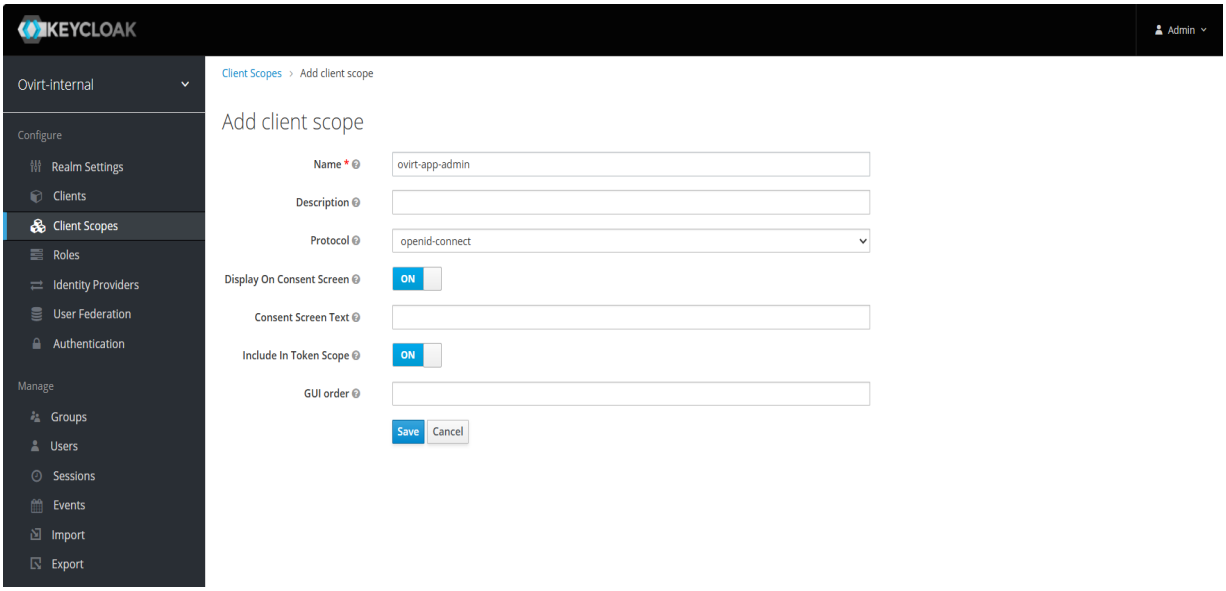

Рисунок 132 –Добавить client scope

3) аналогично добавить client scope (рисунок 133):

– ovirt-app-api;
– ovirt-app-portal;
– ovirt-ext=auth:identity;

– ovirt-ext=auth:sequence-priority=~;
– ovirt-ext=revoke:revoke-all;
– ovirt-ext=token-info:authz-search;
– ovirt-ext=token-info:public-authz-search;
– ovirt-ext=token-info:validate;
– ovirt-ext=token:login-on-behalf;
– ovirt-ext=token:password-access.

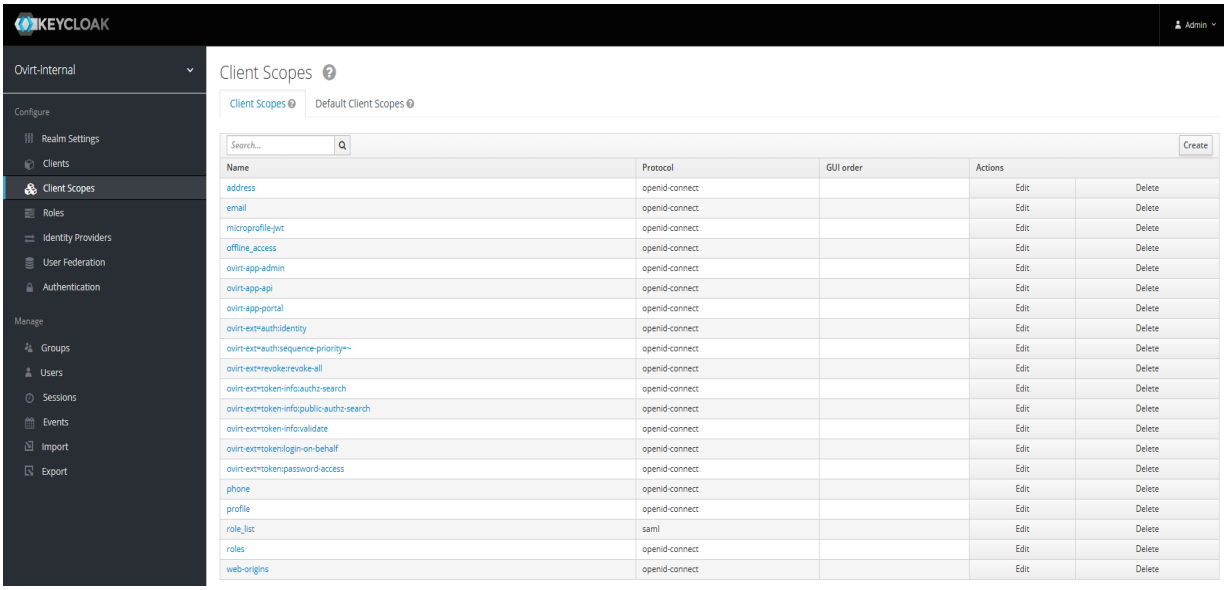

Рисунок 133 –Добавленные client scope

ж) Добавить клиента.

1) перейти в раздел "Clients" и нажать `Create` (рисунок 134).

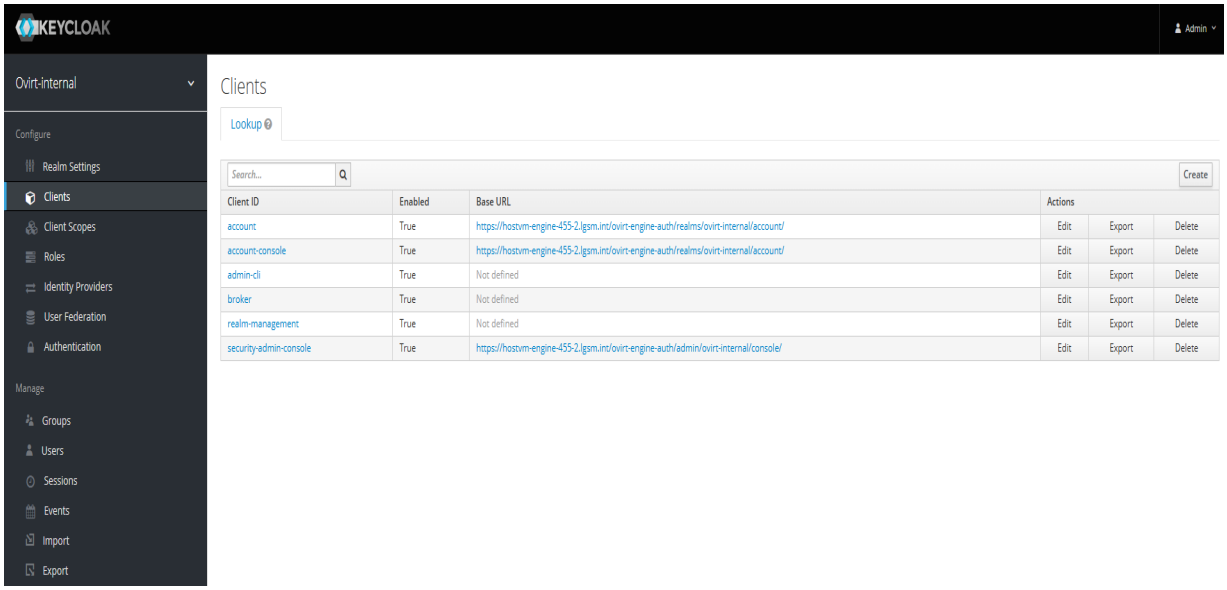

Рисунок 134 –Раздел Clients

2) ввести Client ID: "ovirt-engine-internal" (рисунок 135). В качестве "Root URL" указать "https://FQDN" хоста СУСВ. Ввод подтвердить нажатием кнопки Save.

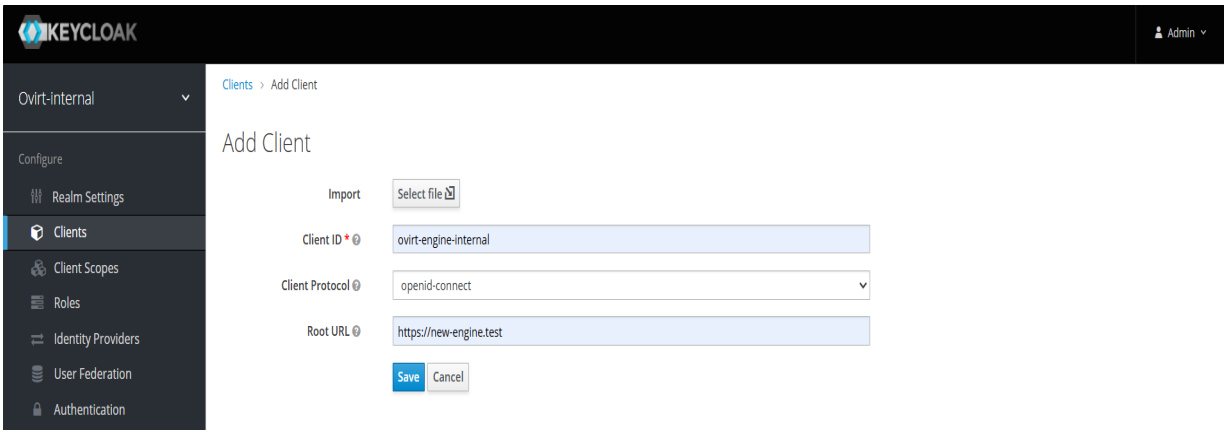

Рисунок 135 –Добавление клиента

Общие настройки клиента выглядят как показано на рисунке 136 и требуют корректировки.

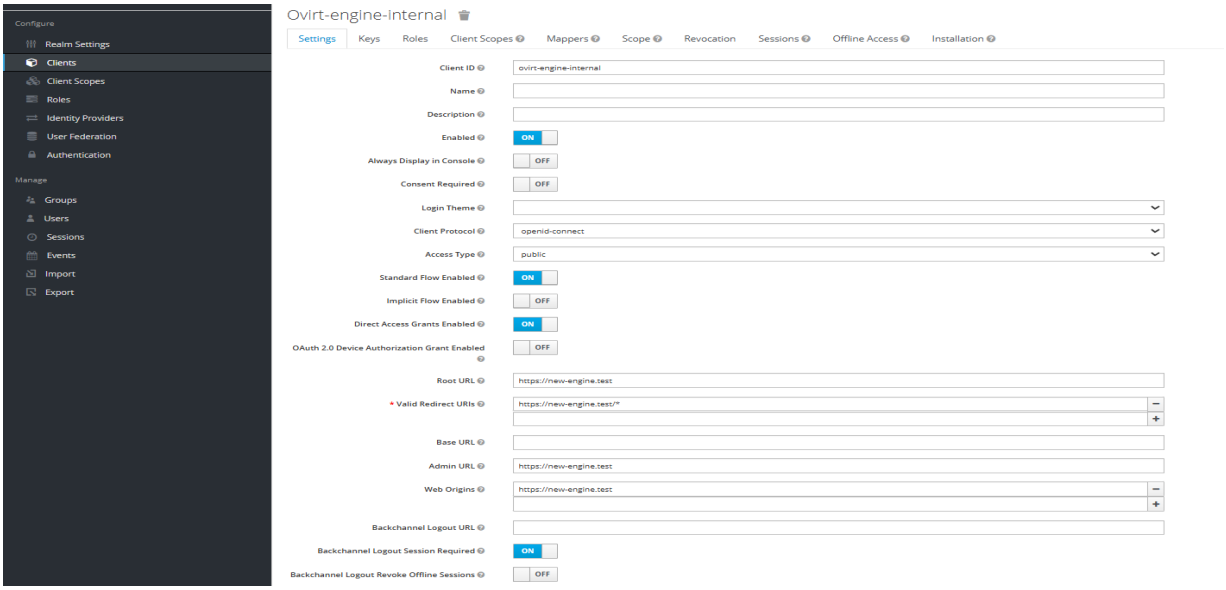

Рисунок 136 –Текущие настройки клиента

3) внести следующие изменения (рисунок 137):

– Access type: confidential;
– Valid Redirect URLs: "https://FQDN/*" изменить на "https://FQDN*";
– Base URL: https://FQDN;
– Backchannel Logout Session Required: OFF,

где FQDN — это доменное имя хоста СУСВ.

Ввод подтвердить нажатием кнопки Save.

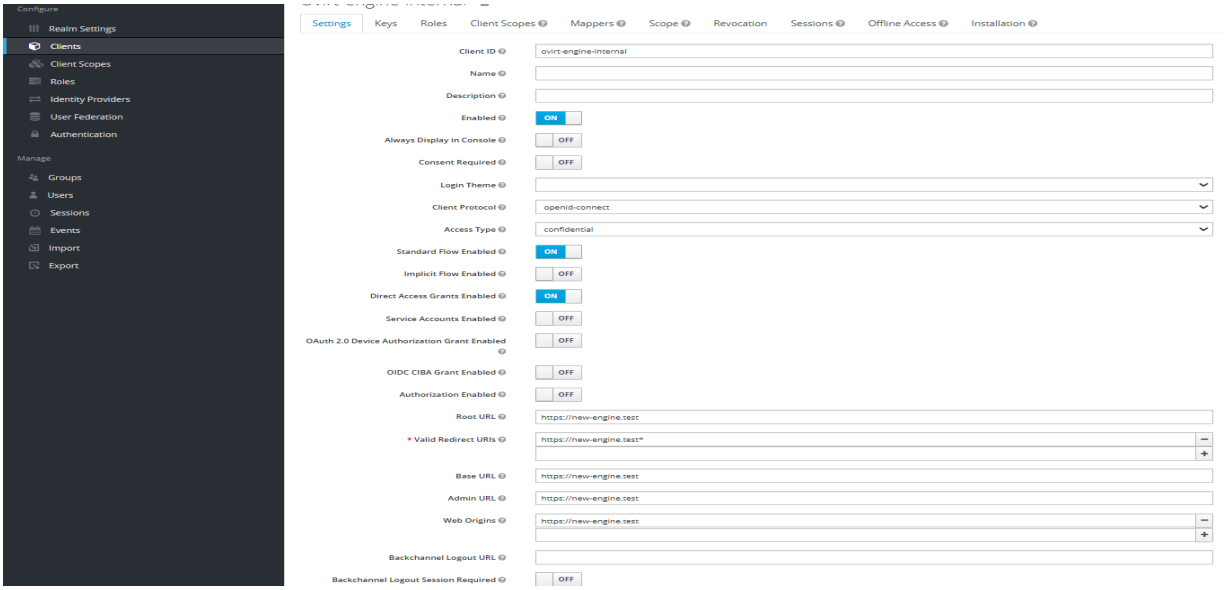

Рисунок 137 –Обновленные настройки клиента

Необходимо обратить внимание, что на вкладке "Credential" раздела "Clients" размещена информация об аутентификации клиента в том числе поле Secret, которое может использоваться при дальнейшей настройке интеграции с сервисом (рисунок 138).

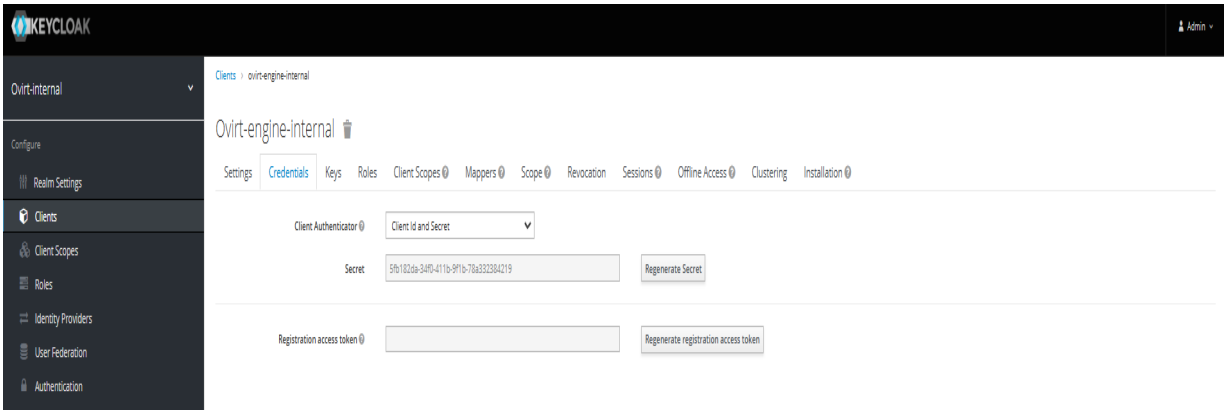

Рисунок 138 –Secret клиента

з) Настроить Client Scopes клиента.

Перейти на вкладку "Client Scopes" раздела "Clients" (рисунок 139).

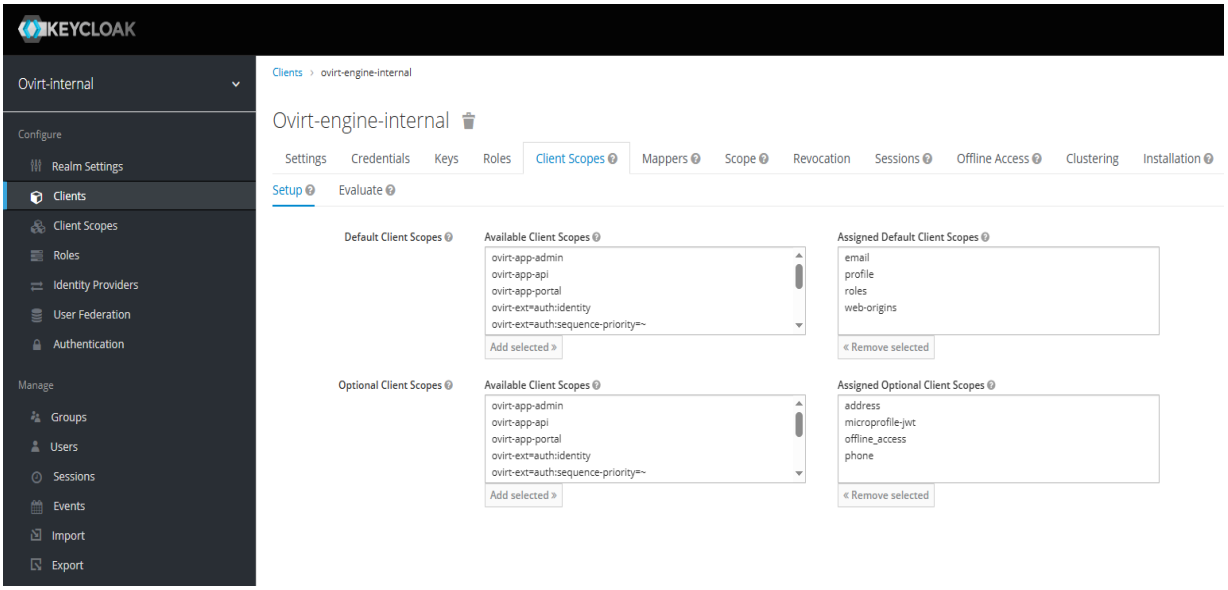

Рисунок 139 – Текущие настройки Client Scopes клиента

Необходимо перевести все доступные "Optional Client Scopes" из "Available Client Scopes" в "Assigned Optional Client Scopes" (рисунок 140).

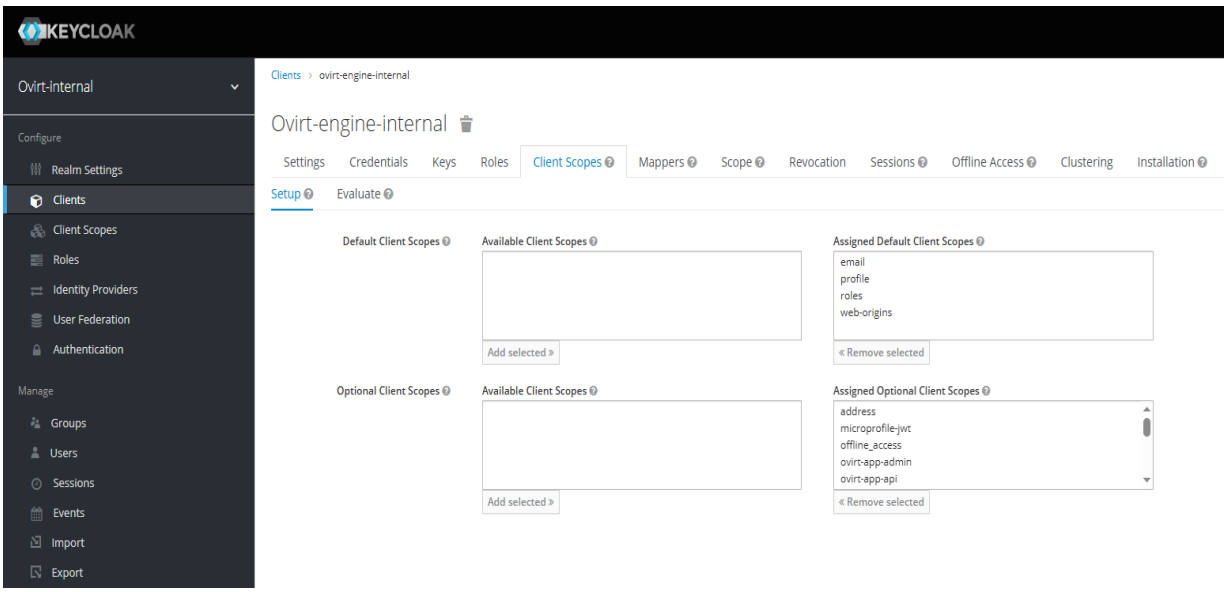

Рисунок 140 – Измененные настройки Client Scopes клиента

и) Добавить клиенту протоколы:

1) перейти на вкладку "Mappers" раздела "Clients" и нажать кнопку `Create` (рисунок 141).

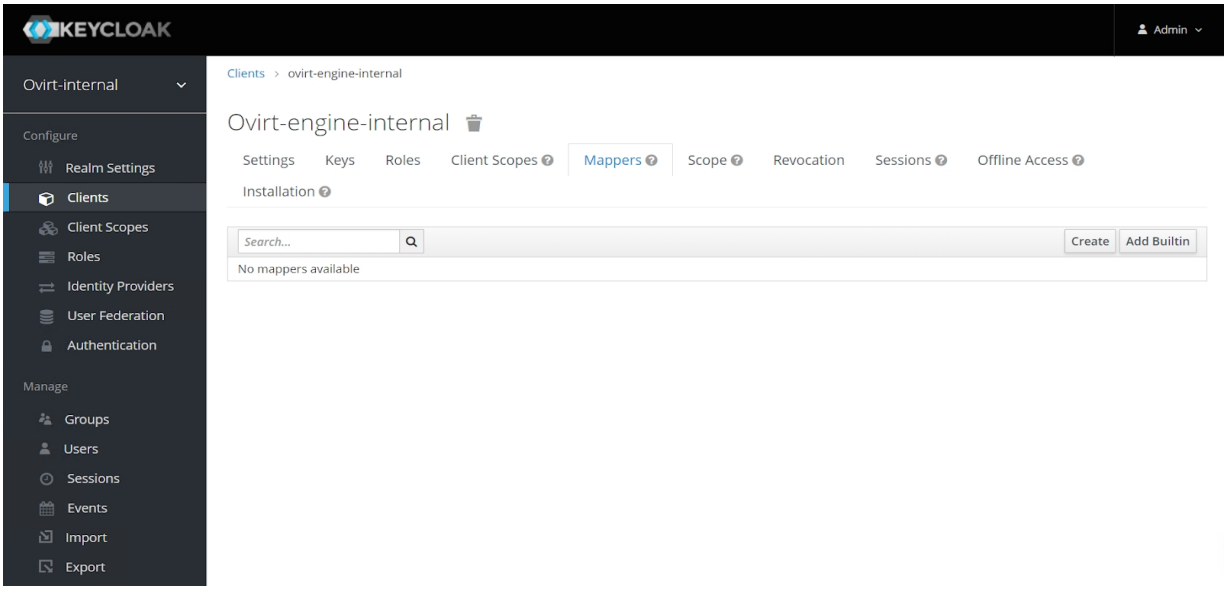

Рисунок 141 – Вкладка Mappers

2) создать протокол username со следующими параметрами (рисунок 142):

– Name: username;
– Mapper Type: User Property;
– Property: username;
– Token Claim Name: preferred_username;
– Claim JSON Type: String.

Ввод подтвердить нажатием кнопки Save.

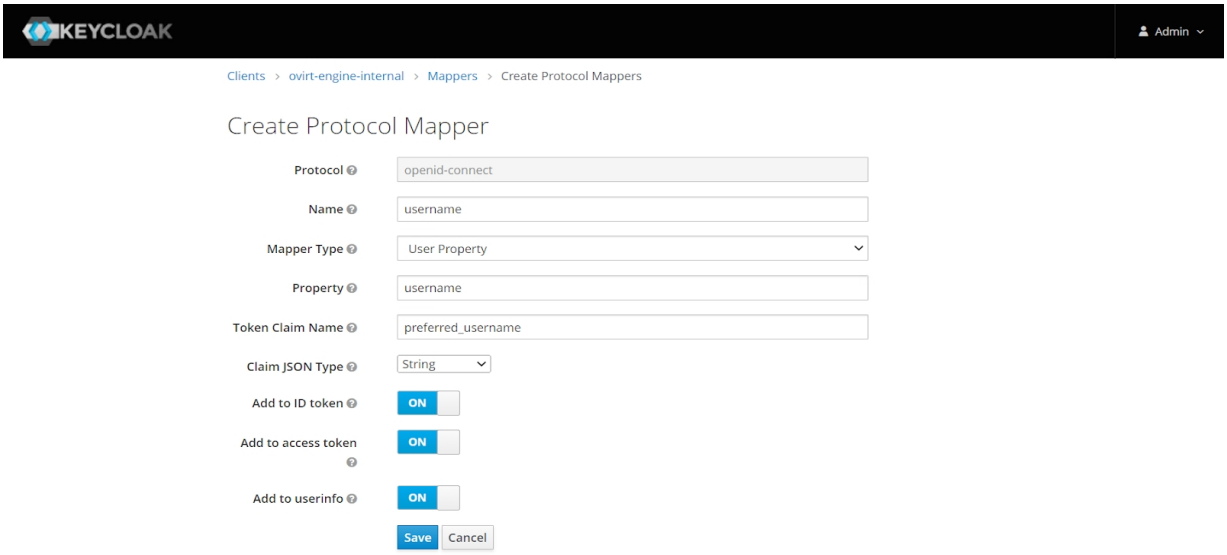

Рисунок 142 – Создание протокола username

3) нажать кнопку `Create` и создать протокол groups со следующими параметрами (рисунок 143):

– Name: groups;
– Mapper Type: Group Membership;
– Token Claim Name: groups.

Ввод завершить нажатием кнопки `Save`.

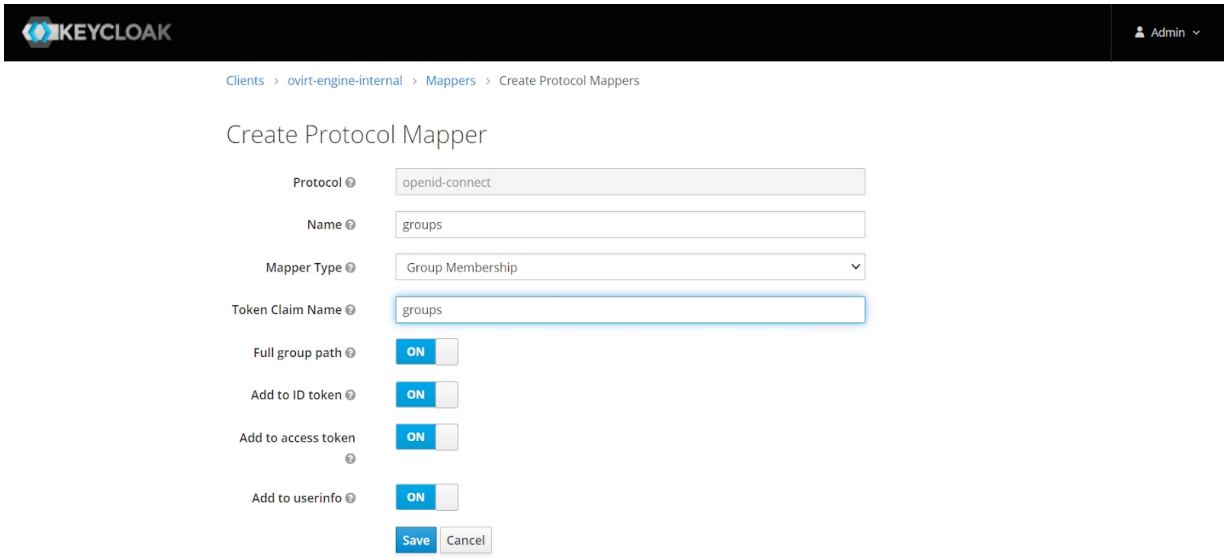

Рисунок 143 – Создание протокола groups

4) нажать кнопку Create и создать протокол realm role со следующими параметрами (рисунок 144):

– Name: realm role;
– Mapper Type: User Realm Role;
– Token Claim Name: realm_access.roles;
– Claim JSON Type: String.

Ввод завершить нажатием кнопки Save.

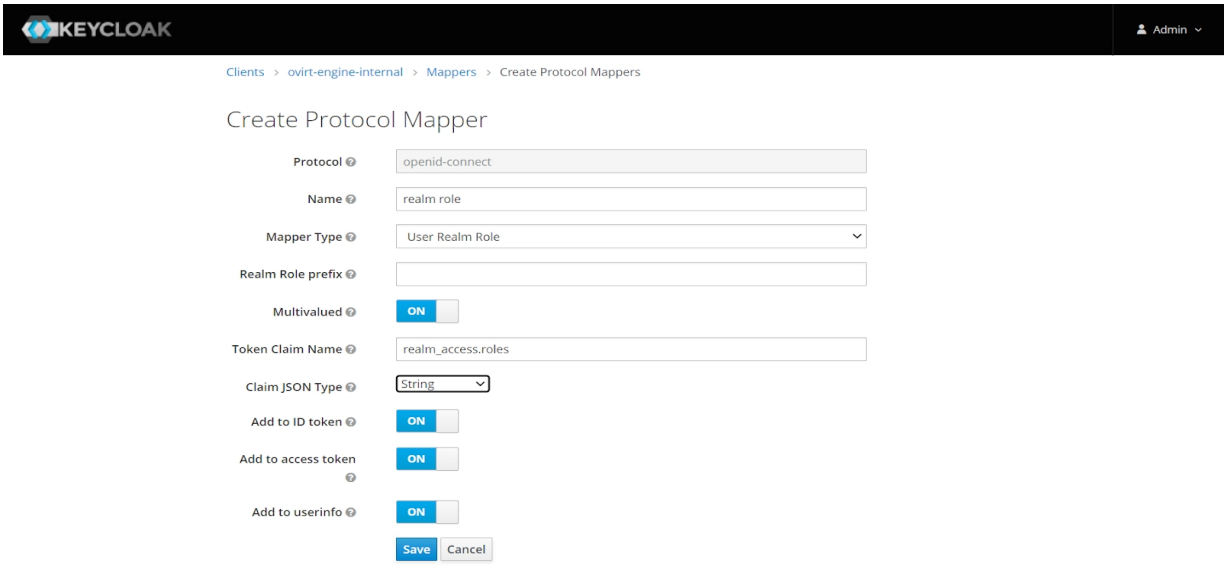

Рисунок 144 – Создание протокола realm role

к) Изменить у клиента срок обновления токена доступа.

Перейти на вкладку "Settings" клиента "ovirt-engine-internal" в разделе "Clients" (рисунок 145). Установить значение параметра Access Token Lifespan 10 дней. Ввод подтвердить нажатием кнопки Save.

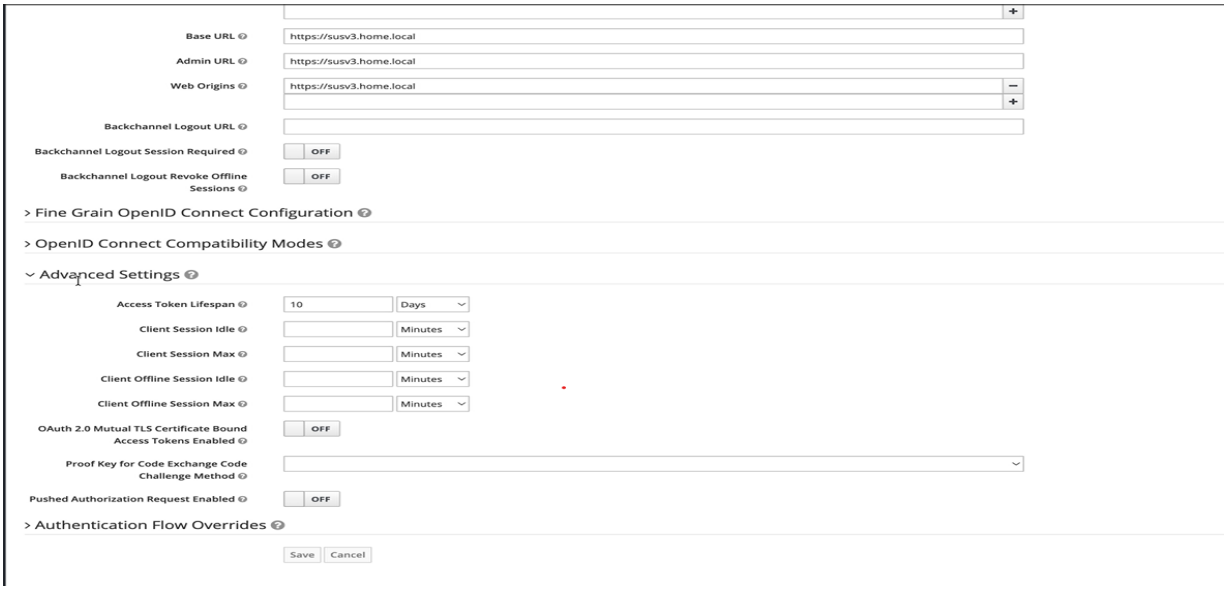

Рисунок 145 – Изменение Access Token Lifespan

На этом настройка параметров Keycloak в административном веб-интерфейсе закончена и необходимо переходить к настройке интеграции на хосте СУСВ.

4.2 Интеграция СУСВ с внешним Keycloak

Модуль интеграции с внешним Keycloak входит в состав интерфейса РОСА Виртуализация и доступен по умолчанию после установки Системы. Установка отдельного дистрибутива или выполнение дополнительных шагов для подключения модуля не требуется.

Для перехода к настройкам интеграции с внешним Keycloak нужно открыть веб-интерфейс Cockpit на виртуальной машине менеджера виртуализации по адресу https://<адрес_менеджера>:9090 (рисунок 146).

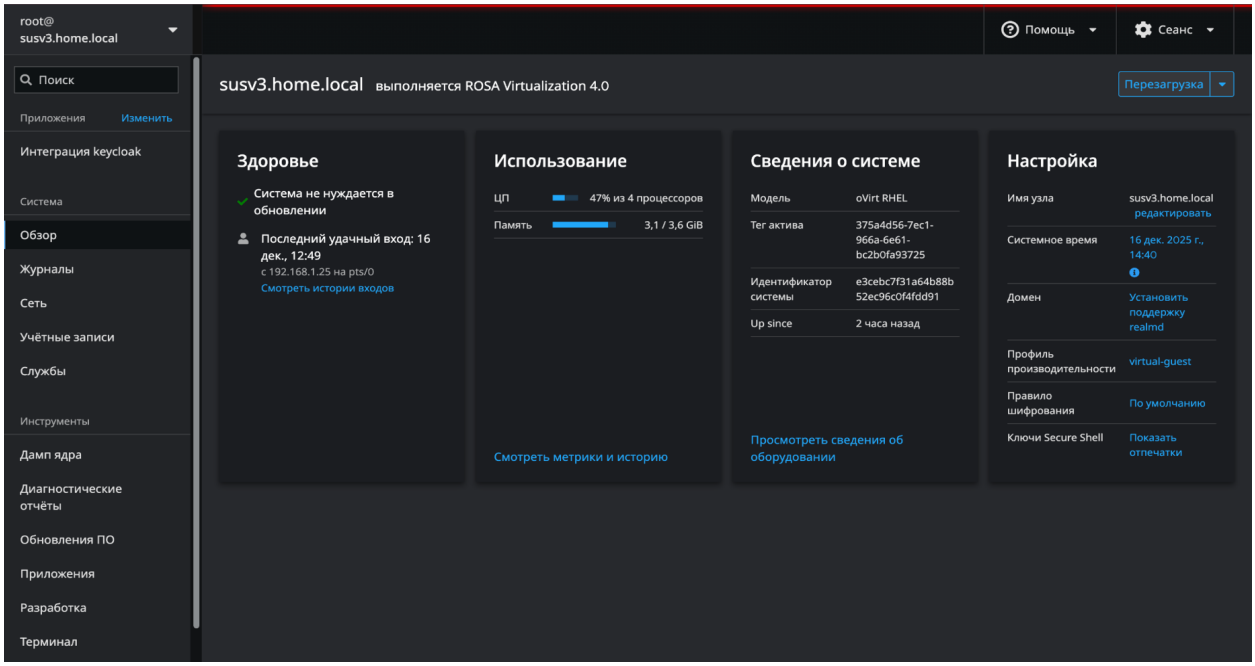

Рисунок 146 – Веб-интерфейс Cockpit

В навигационном меню Cockpit следует выбрать раздел "Интеграция Keycloak", после чего отобразится интерфейс модуля, позволяющий выполнить настройку подключения и проверить его состояние (рисунок 147).

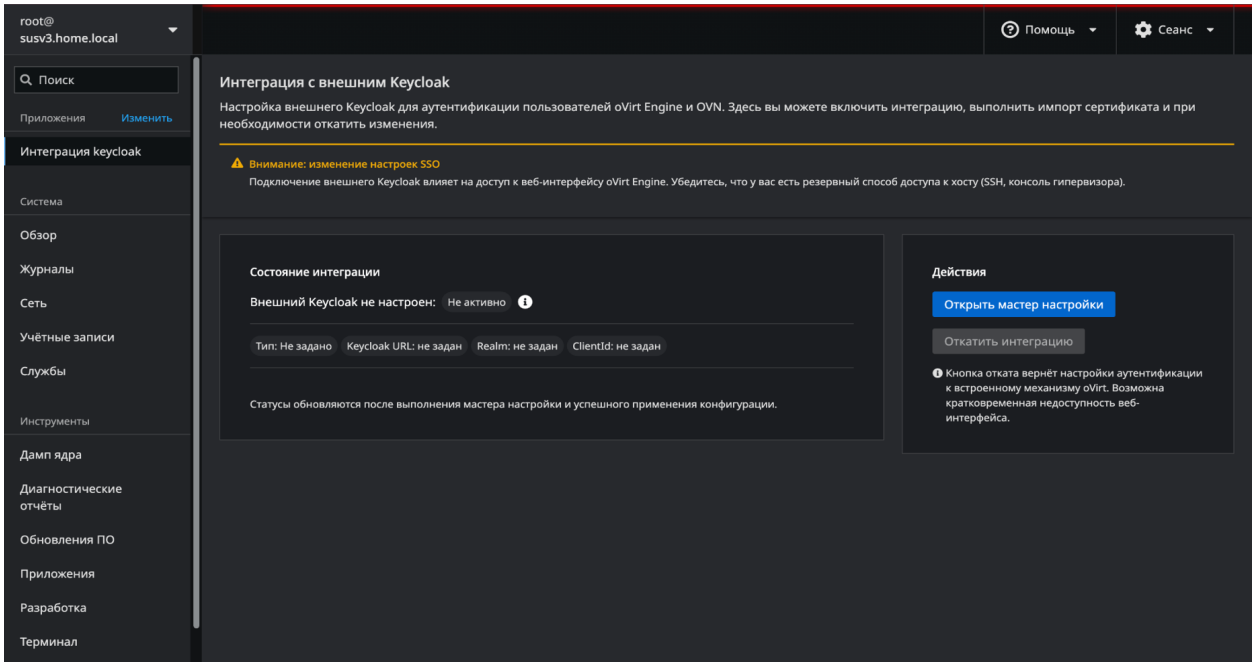

Рисунок 147 – Интеграция с внешним Keycloak

Модуль "Интеграция с внешним Keycloak" предоставляет следующие основные функции:

– Отображение состояния интеграции – отображает текущее состояние интеграции с внешним Keycloak, включая:

– статус активности интеграции (активна/не активна);
– тип подключения(внешняя/внутренняя);
– параметры подключения (URL Keycloak, realm, client ID);
– актуальность и применяемость конфигурации.

– Настройка и активация интеграции – с помощью мастера настройки пользователь может:

– включить интеграцию с внешним Keycloak;
– задать параметры подключения;
– выполнить импорт сертификата;
– применить конфигурацию для oVirt Engine и OVN.

– Откат интеграции – позволяет выполнить откат настроек аутентификации и вернуть встроенный механизм аутентификации Системы, при этом пользователь информируется о возможной кратковременной недоступности веб-интерфейса.

4.2.1 Отображение состояния интеграции

Модуль "Интеграция с внешним Keycloak" отображает текущее состояние механизма аутентификации и параметры подключения.

В зависимости от конфигурации и доступности сервисов возможны три состояния интеграции:

1) Интеграция не настроена (рисунок 148) – в данном состоянии интеграция с внешним Keycloak отсутствует и не активирована.

Характерные признаки состояния:

– отображается статус "Внешний Keycloak не настроен: Не активно";
– параметры подключения отсутствуют;
– поля "Тип", "Keycloak URL", "Realm" и "Client ID" не заданы.

Данное состояние является начальным и соответствует ситуации, когда настройка интеграции ещё не выполнялась.

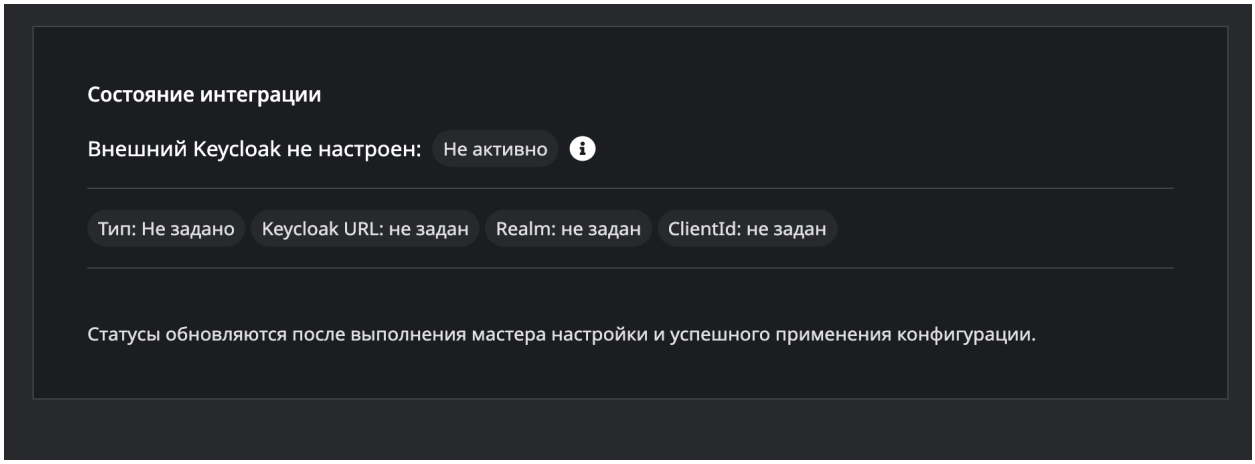

Рисунок 148 – Интеграция с внешним Keycloak не настроена

2) Интеграция активна – в случае успешной настройки и применения конфигурации модуль отображает активное состояние интеграции.

В зависимости от используемого механизма аутентификации возможны два варианта отображения:

– Используется встроенный Keycloak (рисунок 149) – если в системе активен встроенный механизм аутентификации СУСВ, отображается информация о встроенном Keycloak:

– статус "Используется встроенная Keycloak: Активно";
– тип "Встроенная Keycloak";
– отображаются параметры подключения (Keycloak URL, Realm, Client ID);
– выводится предупреждение о невозможности подключения внешнего Keycloak до отключения встроенной интеграции.

Данное состояние означает, что Система использует встроенный механизм аутентификации.

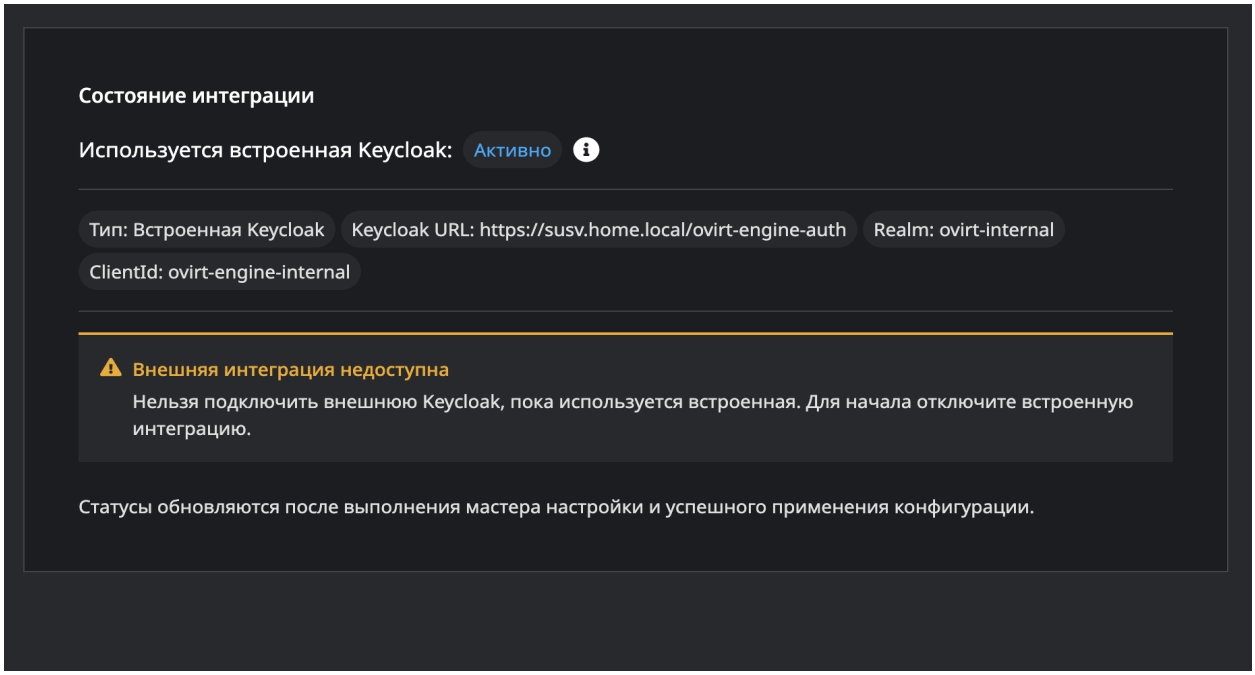

Рисунок 149 – Встроенный Keycloak активен

– Подключён внешний Keycloak (рисунок 150) – если интеграция с внешним сервером Keycloak выполнена успешно, отображается следующее состояние:

– статус "Внешний Keycloak подключён: Активно";
– тип "Внешняя Keycloak";
– отображаются параметры подключения (Keycloak URL, Realm, Client ID).

Это состояние подтверждает, что аутентификация пользователей oVirt Engine и OVN выполняется через внешний сервер Keycloak.

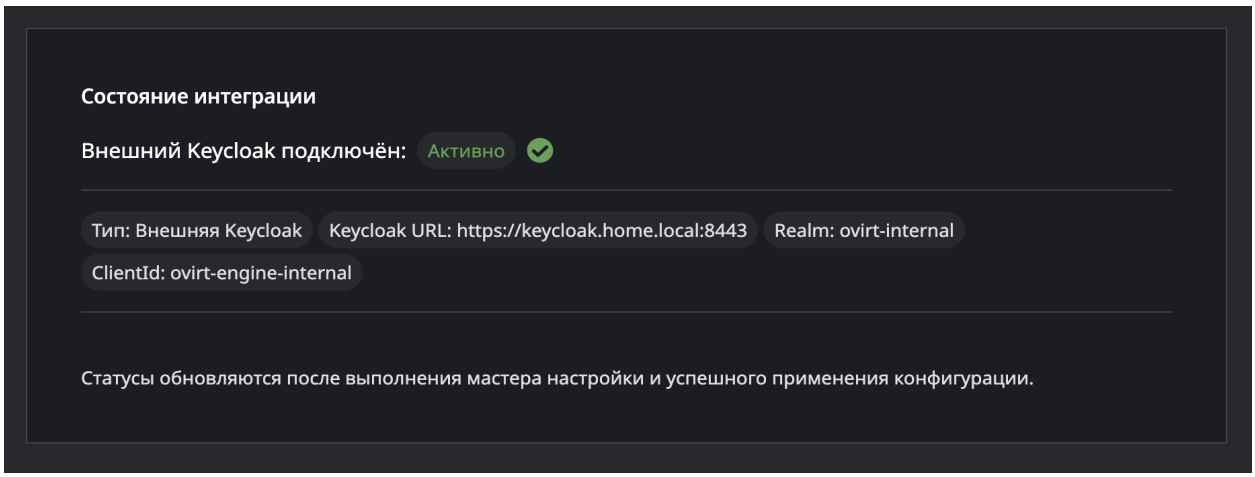

Рисунок 150 – Интеграция с внешним Keycloak активна

3) Ошибка получения состояния интеграции (рисунок 151) – в случае возникновения ошибки при получении данных с серверной части отображается состояние ошибки.

Характерные признаки:

– выводится сообщение "Сервер недоступен";
– отображается уведомление о невозможности получить статус интеграции;
– указывается возможная причина (временная недоступность сервера или проблемы с сетью);
– пользователю рекомендуется обратиться к системному администратору.

Данное состояние не отражает фактическую конфигурацию интеграции и указывает на проблему взаимодействия интерфейса с серверной частью.

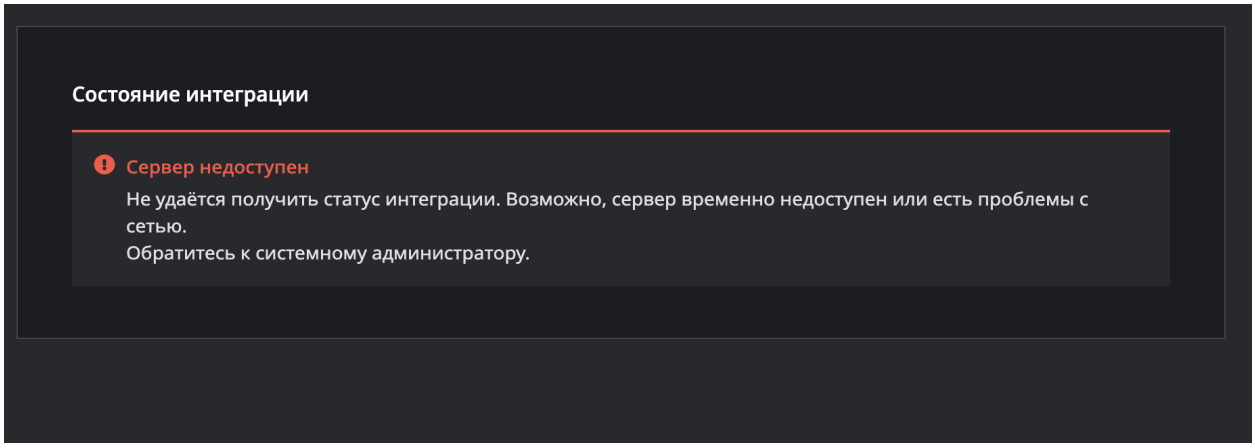

Рисунок 151 – Ошибка получения состояния интеграции

4.2.2 Настройка и активация интеграции

Настройка интеграции выполняется с помощью мастера. Для запуска мастера нужно нажать "Открыть мастер настройки" в разделе интеграции с внешним Keycloak. Начальное окно мастера с четырьмя шагами настроек показано на рисунке 152.

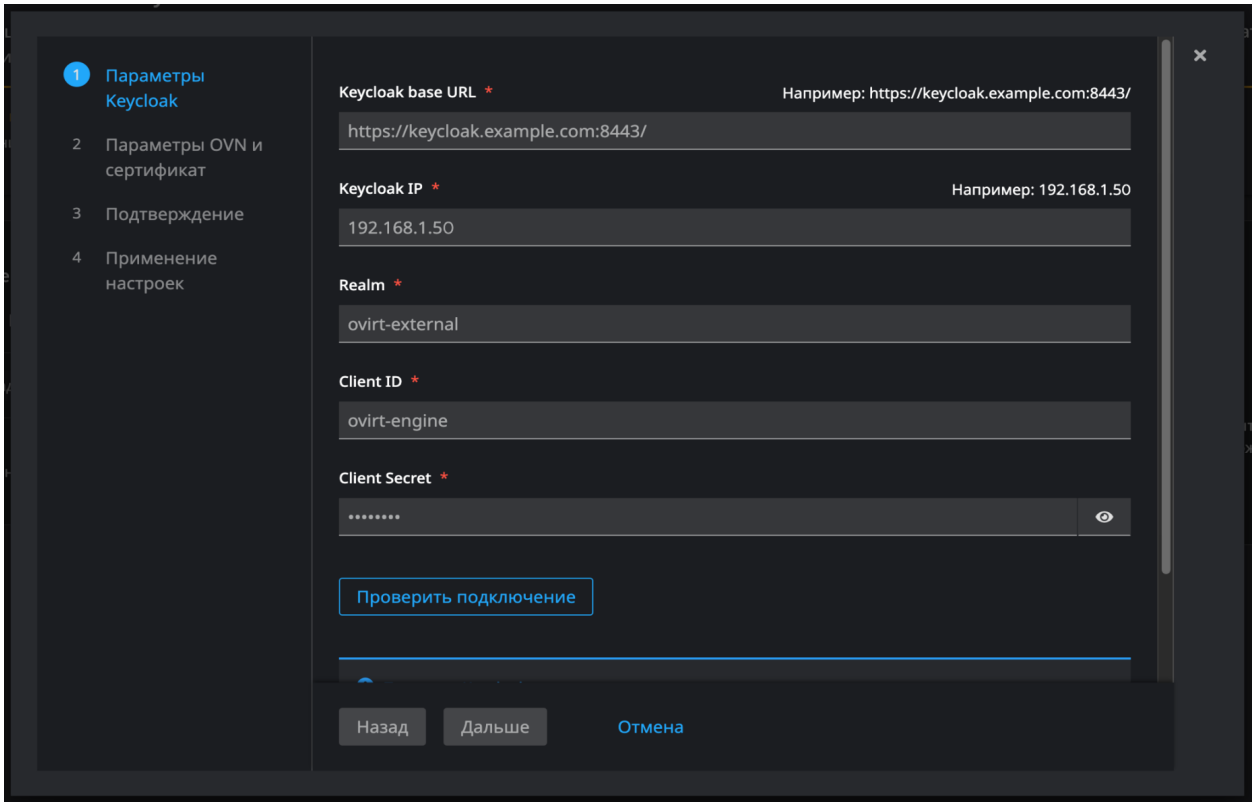

Рисунок 152 – Мастер настройки

4.2.2.1 Шаг 1 – Параметры Keycloak

На первом шаге необходимо указать параметры подключения к серверу Keycloak и данные клиента, через который будет выполняться интеграция.

Обязательные поля:

– Keycloak base URL — базовый URL внешнего Keycloak, например https://keycloak.example.com:8443/;
– Keycloak IP — IP-адрес сервера Keycloak;
– Realm — имя Realm в Keycloak;
– Client ID — идентификатор клиента в Keycloak;
– Client Secret — секрет клиента (отображается скрыто).

При необходимости можно показать/скрыть значение с помощью пиктограммы просмотра.

До запуска проверки отображается информационное сообщение "Проверка Keycloak не выполнялась" с рекомендацией нажать кнопку проверки после ввода параметров.

После заполнения параметров следует нажать кнопку Проверить подключение, чтобы убедиться, что:

– сервер Keycloak доступен по указанному адресу;
– указанные Realm и параметры клиента корректны;
– возможна аутентификация через Client ID/Client secret (если включены необходимые настройки клиента).

Если все параметры указаны корректно и проверка выполнена успешно, отображается сообщение "Keycloak успешно проверен" (рисунок 153). В этом случае становится доступен переход к следующему шагу мастера по кнопке Дальше.

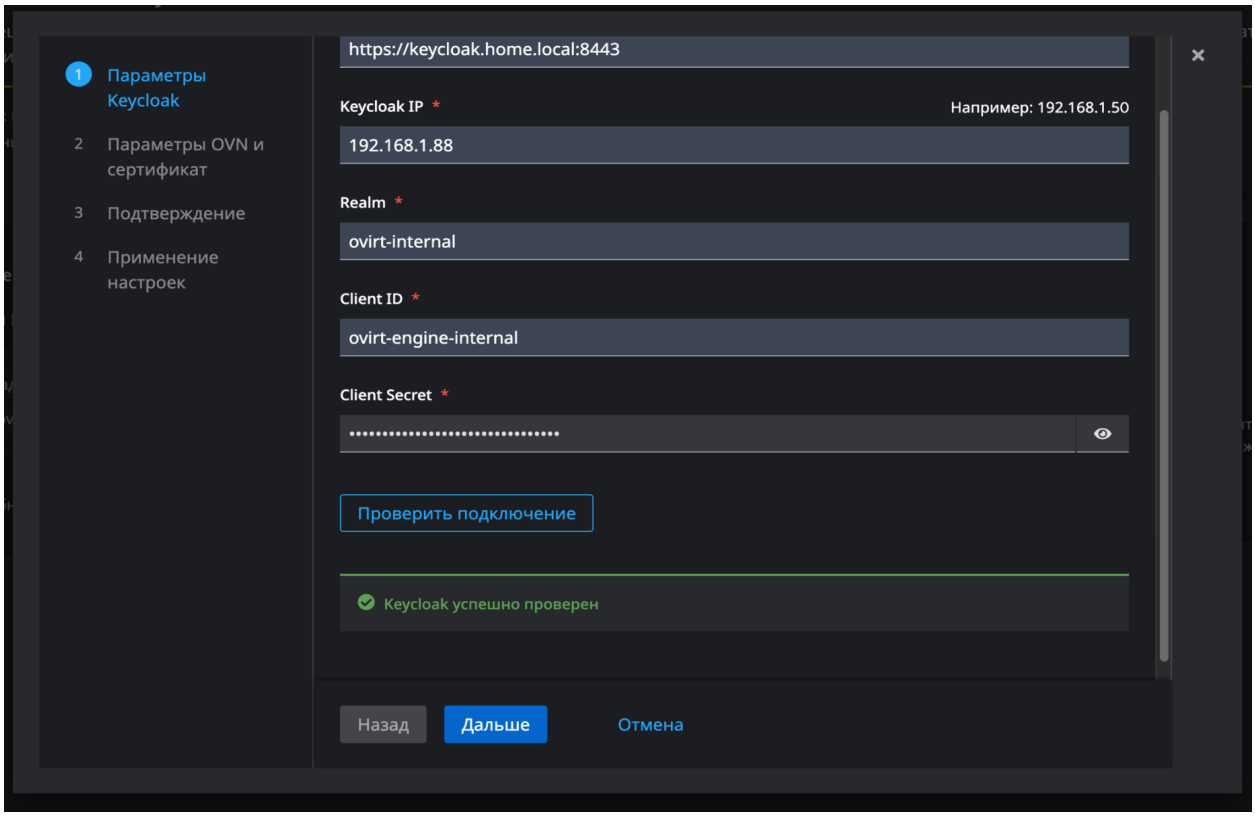

Рисунок 153 – Успешная проверка Keycloak

Если соединение с Keycloak установлено, но часть проверки выполнить не удалось, отображается сообщение "Проверка выполнена с предупреждением" (рисунок 154).

Типовой случай в качестве примера: для клиента отключены Service Accounts, из-за чего невозможно подтвердить корректность Client ID и Client Secret, а в сообщении отображается рекомендация включить Service Accounts в настройках клиента Keycloak.

Примечание – Возможно продолжение настройки, но при дальнейшей интеграции могут возникнуть ошибки, связанные с правами клиента или невозможностью получить сервисный токен.

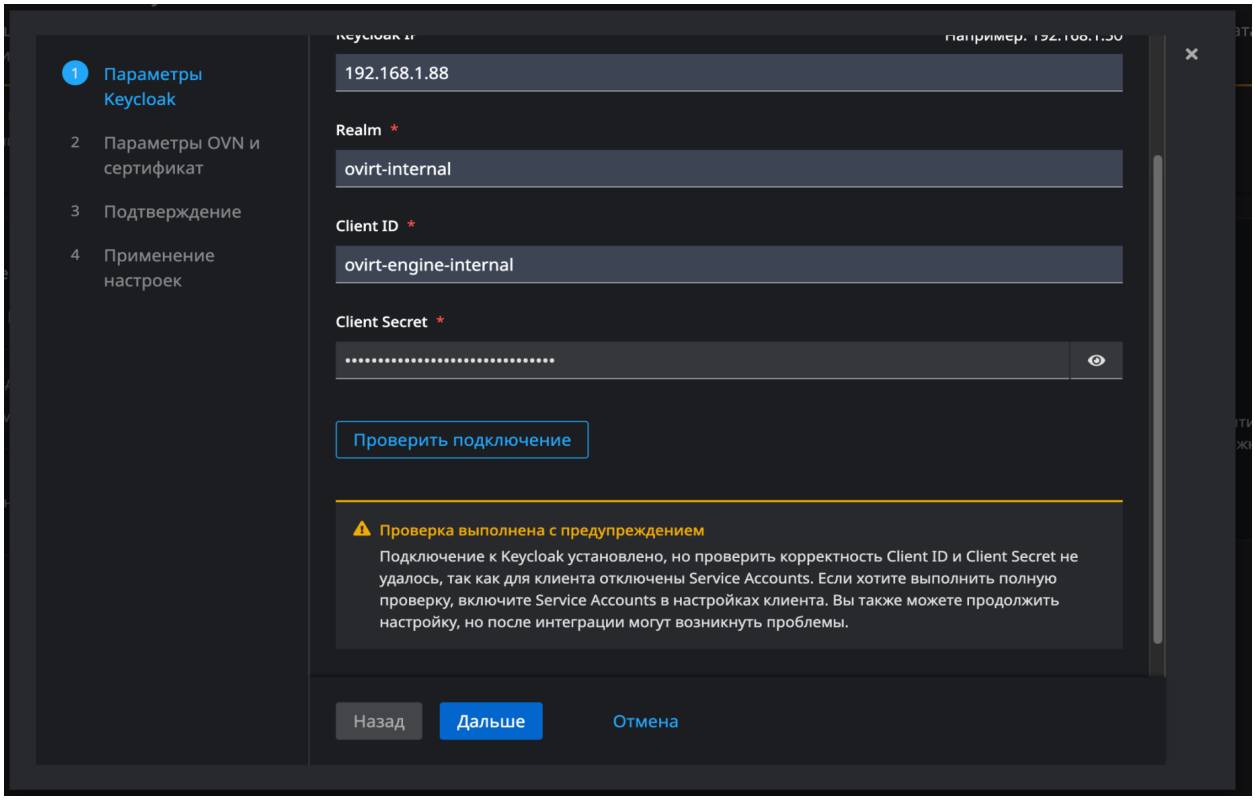

Рисунок 154 – Проверка выполнена с предупреждением

Если успешно выполнить проверку не удалось, отображается сообщение "Не удалось проверить Keycloak" (рисунок 155).

Возможные причины:

– указан неверный URL или IP Keycloak;
– сервер Keycloak недоступен по сети;
– некорректно указаны Realm, Client ID или Client secret;
– используется неверный протокол/порт (например, ожидается HTTPS, но доступен только HTTP).

В этом случае необходимо проверить введённые параметры и повторить проверку подключения.

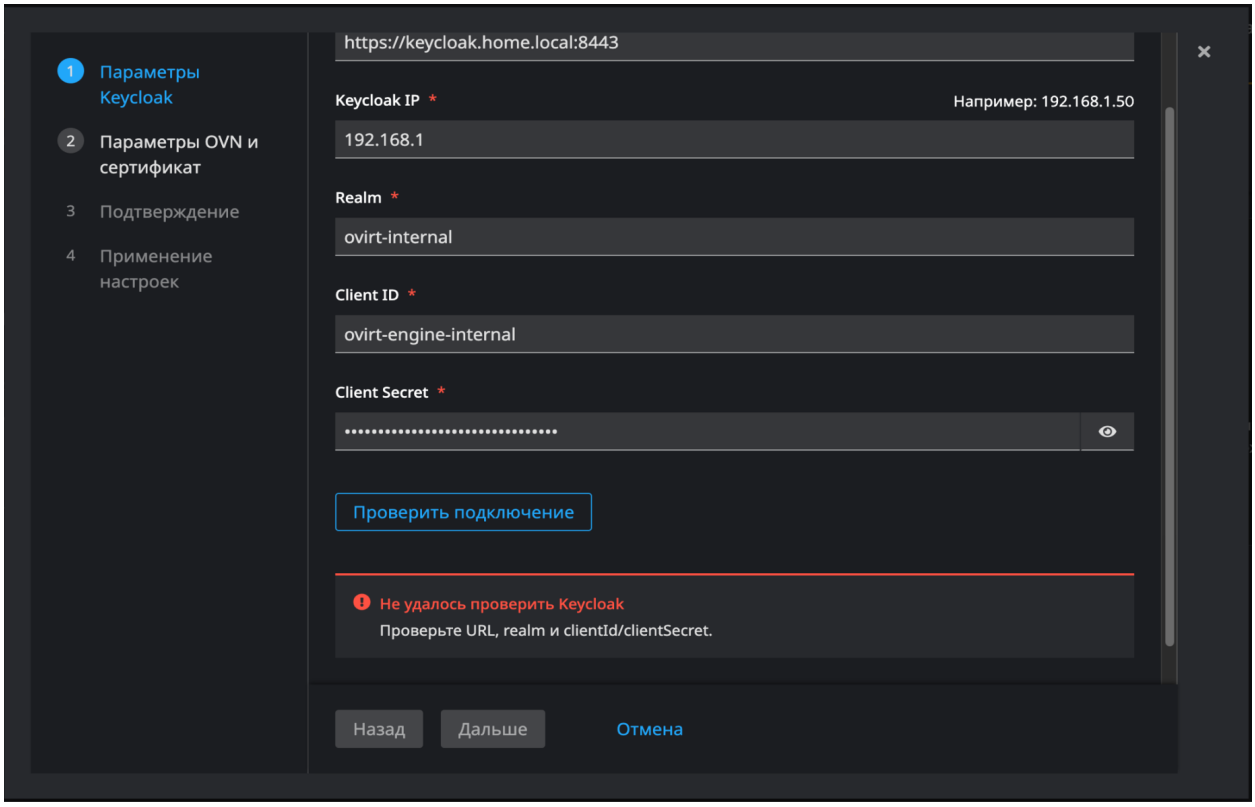

Рисунок 155 – Проверка не удалась

4.2.2.2 Шаг 2 – Параметры OVN и сертификат

На втором шаге мастера выполняется настройка параметров OVN и импорт сертификата Keycloak, необходимого для корректного взаимодействия сервисов ovirt-provider-ovn и механизма SSO (рисунок 156).

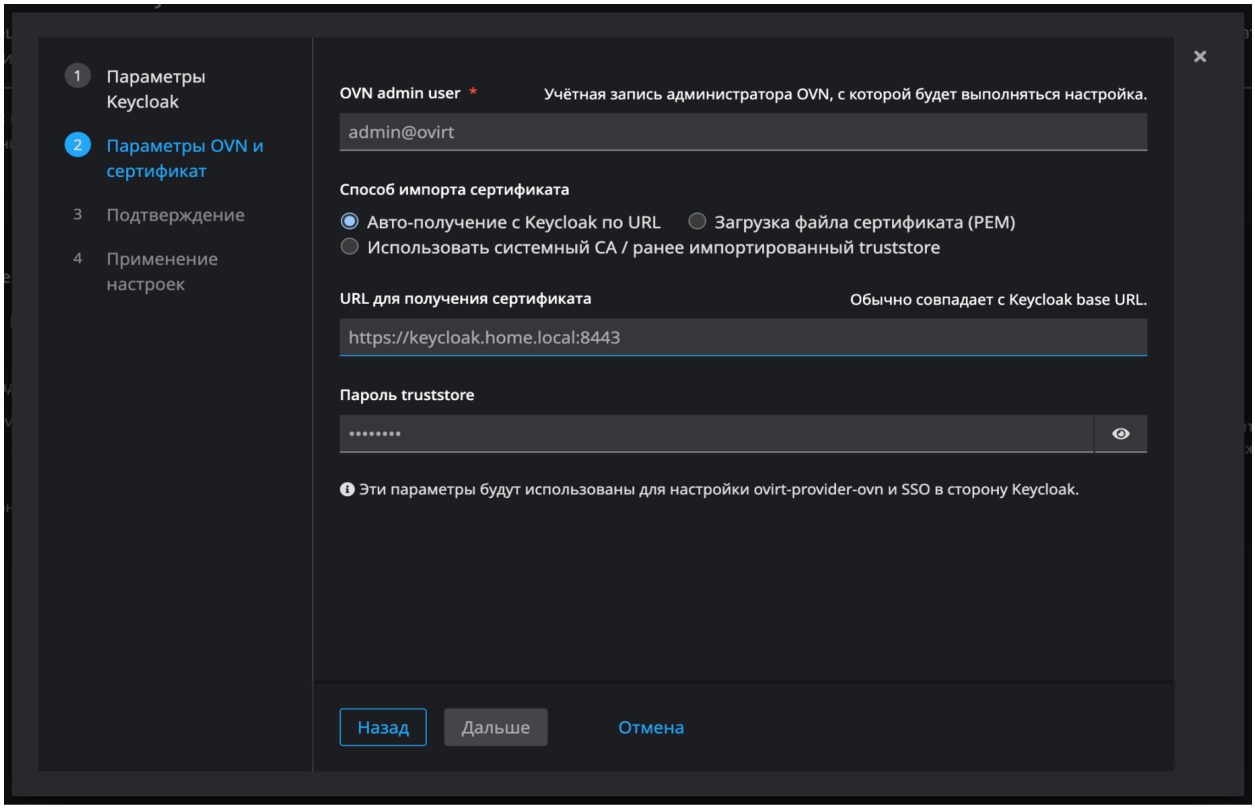

Рисунок 156 – Параметры OVN и сертификат

Параметры OVN для настройки:

– OVN admin user — учётная запись администратора OVN, от имени которой будет выполняться настройка интеграции. Указанный пользователь должен обладать необходимыми правами для применения конфигурации.

– Способ импорта сертификата – для доверенного взаимодействия с сервером Keycloak необходимо наличие корректного TLS-сертификата. Модуль поддерживает три способа импорта сертификата:

1) Автоматическое получение сертификата с Keycloak по URL – сертификат автоматически запрашивается с сервера Keycloak по указанному адресу "URL для получения сертификата", который, как правило, совпадает со значением "Keycloak base URL", указанным на первом шаге. Этот способ рекомендуется использовать, если:

– сервер Keycloak доступен по сети;
– используется стандартная TLS-конфигурация;
– нет необходимости в ручном управлении сертификатами.

2) Загрузка файла сертификата (PEM) – сертификат загружается вручную в виде файла. Допустимы следующие форматы файлов сертификатов: .pem, .crt, .cer, .txt. Возможные ошибки при загрузке:

– Недопустимый формат файла – если выбран файл неподдерживаемого типа, отображается сообщение: "Недопустимый формат файла. Разрешены файлы сертификатов (.pem, .crt, .cer, .txt).";

– Некорректный сертификат PEM – если файл имеет допустимое расширение, но его содержимое не соответствует формату PEM (повреждённый файл или неверная структура), отображается сообщение "Файл не является корректным сертификатом в формате PEM.".

В обоих случаях необходимо выбрать корректный файл сертификата и повторить загрузку.

3) Использовать системный CA / ранее импортированный truststore – используется сертификат, уже присутствующий в системном truststore или доверенный системным центром сертификации (CA). Этот способ рекомендуется, если:

– сертификат Keycloak уже был импортирован ранее;
– используется корпоративный или системный CA;
– нет необходимости повторно добавлять сертификат.

Поле "Пароль truststore" — пароль для доступа к хранилищу доверенных сертификатов – является обязательным для всех способов импорта и используется при применении конфигурации.

Примечание – Указанные на данном шаге параметры будут использованы для настройки ovirt-provider-ovn и механизма SSO в сторону Keycloak.

4.2.2.3 Шаг 3 – Подтверждение

На третьем шаге мастера пользователю отображается предупреждение и краткое резюме конфигурации, которая будет применена к Системе (рисунок 157).

В верхней части экрана отображается предупреждающее сообщение "Внимание: изменение настроек аутентификации". В предупреждении указывается, что:

– подключение внешнего Keycloak изменяет механизм аутентификации oVirt Engine;
– при ошибке конфигурации веб-интерфейс может стать недоступен;
– рекомендуется заранее обеспечить альтернативный доступ к хосту Engine (например, по SSH) для возможности ручного отката настроек.

Также на этом шаге в окне отображается краткое резюме конфигурации со сводной информацией по всем параметрам, заданным на предыдущих шагах мастера.

Под резюме отображается информационное сообщение о том, что после завершения мастера будут:

– обновлены конфигурационные файлы ovirt-engine;
– обновлена конфигурация ovirt-provider-ovn;
– при необходимости обновлён truststore.

Для продолжения настройки необходимо нажать кнопку Подключить, после чего мастер перейдёт к шагу применения настроек.

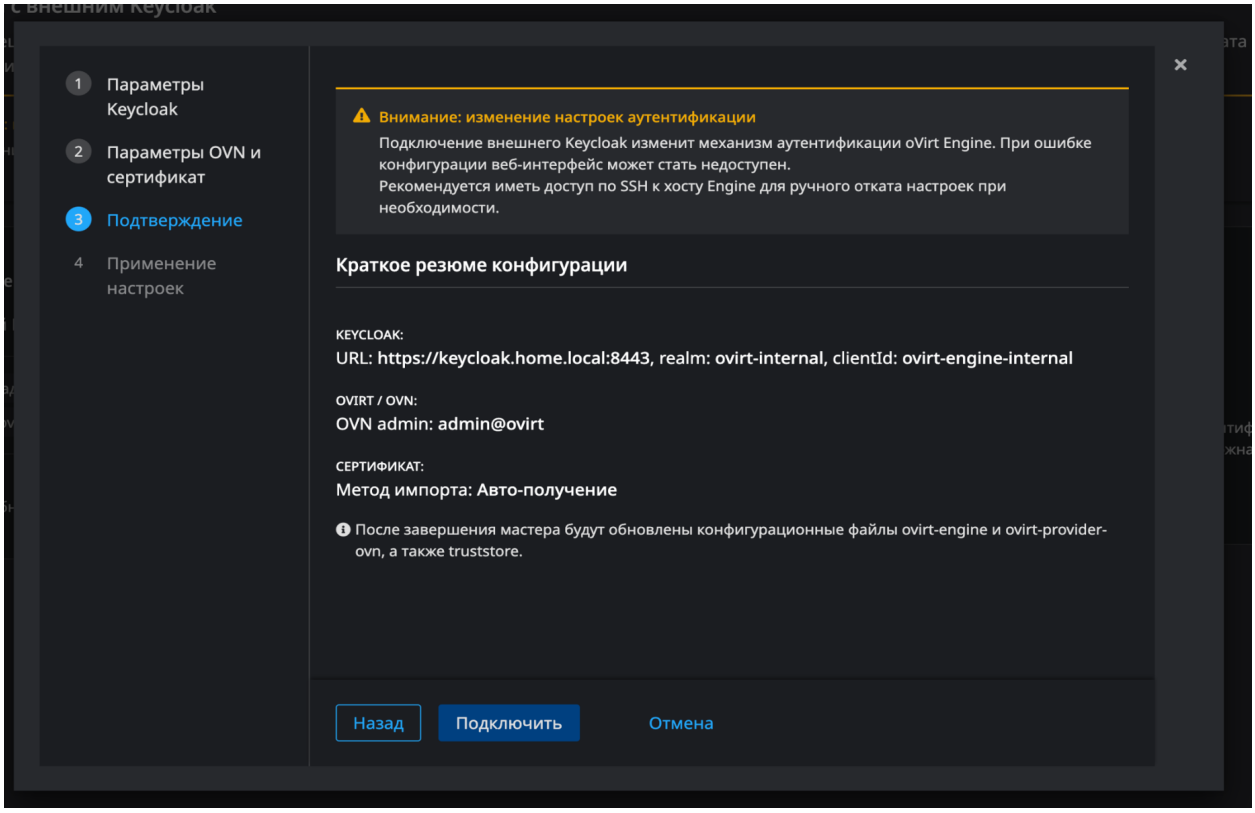

Рисунок 157 – Этап подтверждения

4.2.2.4 Шаг 4 – Применение настроек

На четвёртом шаге мастера выполняется непосредственное применение конфигурации и запуск процесса интеграции с внешним Keycloak.

После подтверждения параметров система автоматически начинает процесс настройки. В интерфейсе отображается информационное сообщение "Выполняется интеграция с внешней Keycloak..." (рисунок 158).

В этот момент выполняются следующие действия:

– обновляются конфигурационные файлы ovirt-engine;
– настраивается интеграция ovirt-provider-ovn;

– производится настройка и обновление truststore;
– применяется механизм аутентификации через внешний Keycloak;
– перезапускаются сервисы.

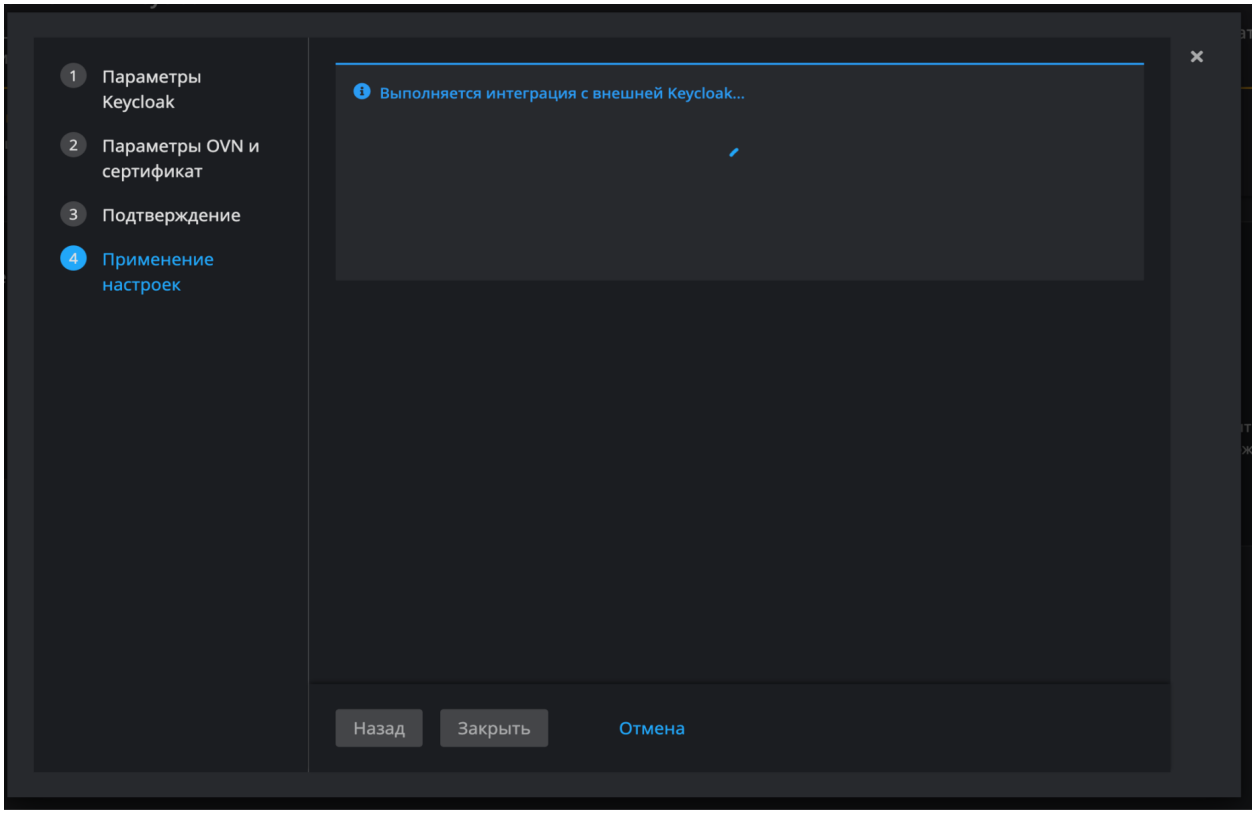

Рисунок 158 – Процесс интеграции

В случае успешного применения конфигурации отображается сообщение "Интеграция с внешней Keycloak успешно выполнена" (рисунок 159).

После этого работу с мастером можно завершить, нажав кнопку Закрыть.

В результате в разделе "Состояние интеграции" будет отображаться активная интеграция с внешним Keycloak.

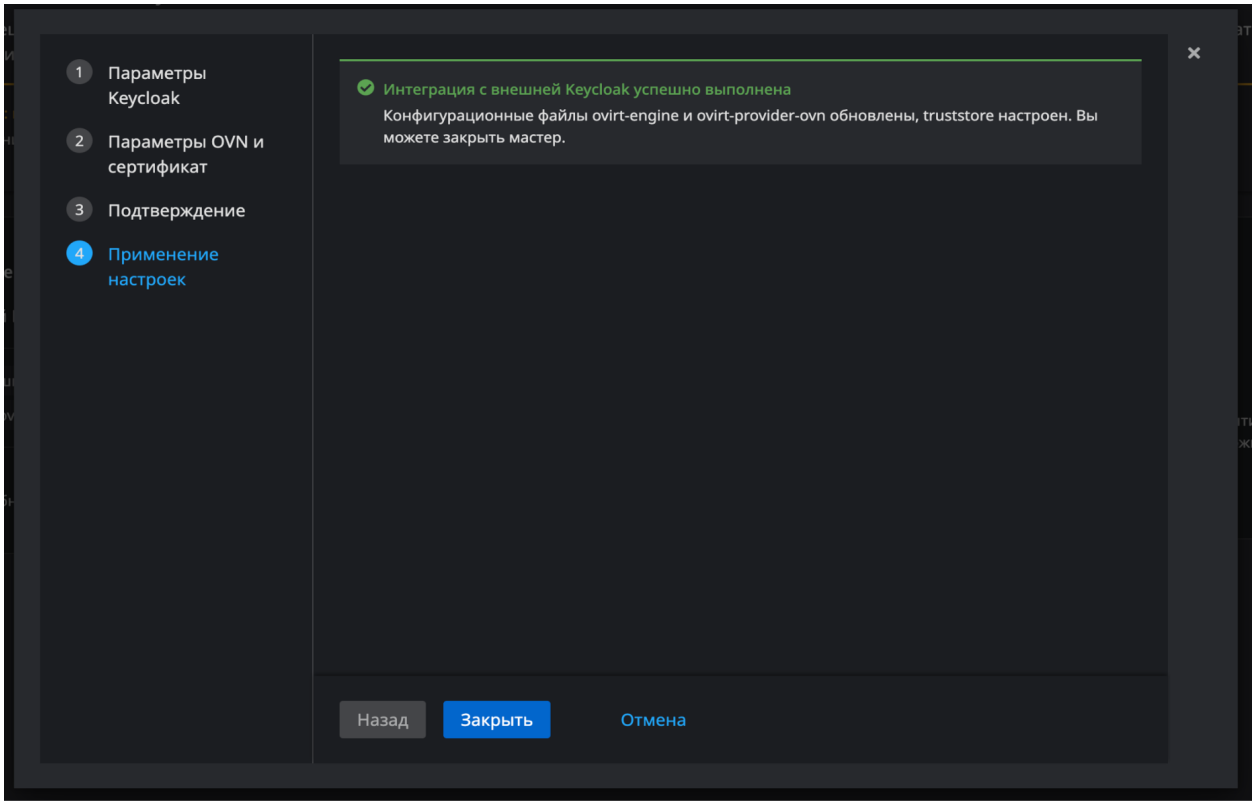

Рисунок 159 – Интеграция успешна

Если в процессе применения конфигурации возникает ошибка, отображается сообщение "Ошибка при выполнении интеграции", и в блоке сообщения указываются (рисунок 160):

– общее описание ошибки;

– подробная информация о причине (например, ошибка импорта сертификата, неверный пароль truststore и т. д.).

Рекомендации по устранению ошибки:

а) внимательно изучить текст ошибки и её детали;

б) вернуться на шаг мастера, на котором была допущена ошибка (например, параметры Keycloak или параметры сертификата);

в) исправить значение поля, указанного в сообщении об ошибке;

г) повторить применение настроек.

При необходимости рекомендуется дополнительно проверить логи keycloak-connect для более детального анализа причины сбоя.

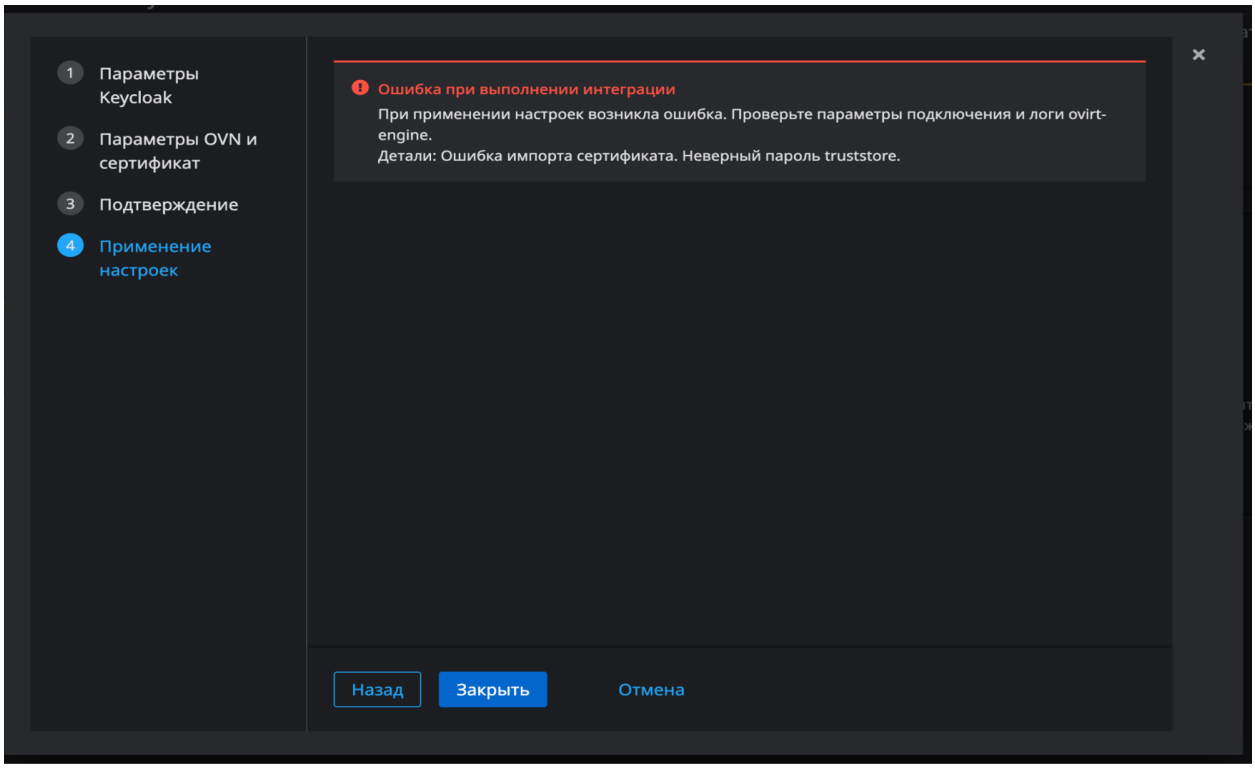

Рисунок 160 – Ошибка при выполнении интеграции

4.2.3 Откат интеграции

Функция отката интеграции предназначена для восстановления предыдущих настроек аутентификации в случае возникновения проблем после подключения внешнего Keycloak. Процедура отказа запускается нажатием кнопки `Откатить интеграцию` в основном окне "Интеграция с внешним Keycloak". В открывшемся диалоговом окне необходимо подтвердить действие, нажав кнопку `Откатить интеграцию` (рисунок 161).

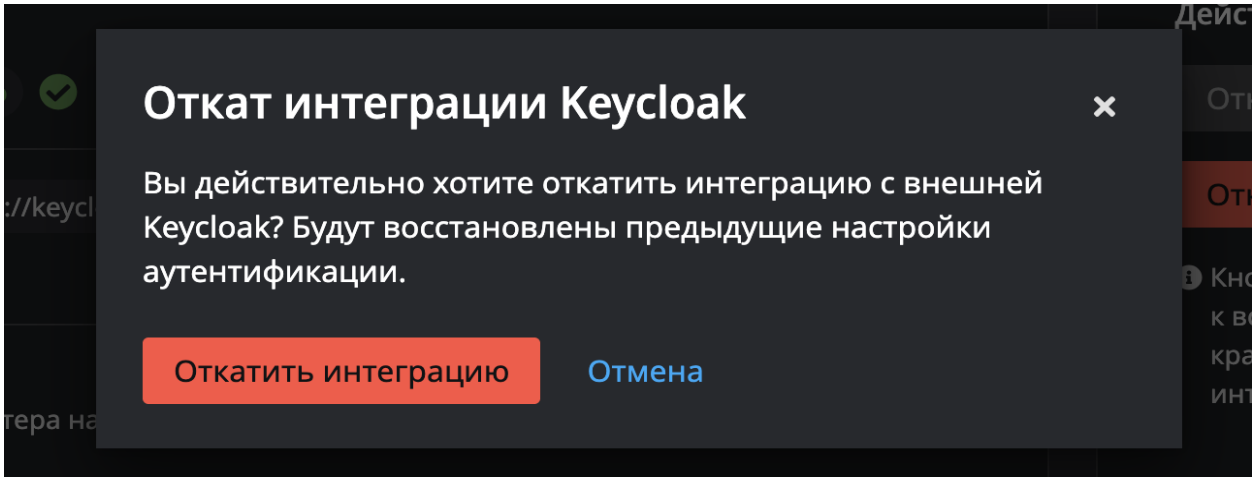

Рисунок 161 – Подтверждение отката интеграции

Откат рекомендуется выполнять в следующих ситуациях:

– После успешной установки интеграции веб-интерфейс менеджера виртуализации становится недоступен.

– Возникают ошибки в работе сервиса ovirt-provider-ovn.

– Изменились или стали некорректными параметры внешнего Keycloak (URL, Realm, Client, сертификаты).

– Требуется временно вернуть встроенный механизм аутентификации Системы.

Откат позволяет безопасно вернуться к состоянию, которое использовалось до подключения внешнего Keycloak.

После подтверждения выполнения отката:

а) модальное окно закрывается;

б) в разделе "Состояние интеграции" отображается индикатор загрузки, указывающий на выполнение операции отката (рисунок 162);

в) выполняется восстановление конфигурации аутентификации и связанных компонентов.

Во время выполнения операции возможна кратковременная недоступность веб-интерфейса.

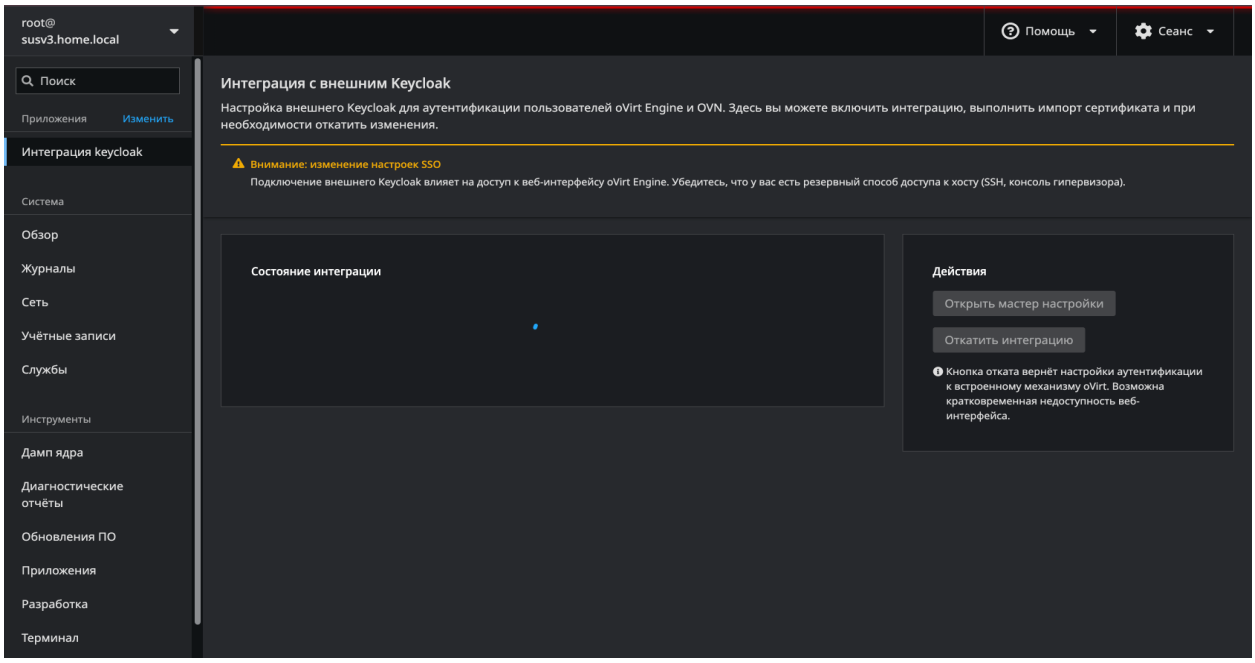

Рисунок 162 – Процесс отката

При успешном завершении отката:

– в разделе "Состояние интеграции" отображается состояние, соответствующее варианту "Интеграция не настроена";

– Система возвращается к предыдущему механизму аутентификации;

– внешний Keycloak больше не используется для аутентификации.

4.3 Управление доступом в СУСВ интегрированном с внешним Keycloak

После подключения интеграции Keycloak становится единственным механизмом идентификации пользователей и управления доступом в СУСВ.

Механизм единого входа Keycloak дает возможность пользователям войти в Портал ВМ, Портал администрирования или Портал мониторинга без повторного ввода пароля. Данные учетной записи для аутентификации получаются с сервера Keycloak.

Примечание — При активированном едином входе на Портал ВМ невозможен единый вход в виртуальные машины. При активированном едином входе на Портал ВМ в пароле нет необходимости, поэтому невозможно передать этот пароль для входа в Систему на ВМ.

Для обеспечения доступа пользователя в СУСВ необходимо в Keycloak создать учетные записи. Пользователи и группы создаются в интерфейсе Keycloak, затем в Портале администрирования СУСВ необходимо назначить им соответствующие права доступа.

Примечание — Ранее созданные в СУСВ локальные аккаунты, в том числе учетная запись admin@internal, имеющая полные административные права в СУСВ, становятся недоступными. Но в случае отката интеграции все ранее настроенные аккаунты будут доступны и работоспособны.

В режиме интеграции подключение служб каталогов к СУСВ не поддерживается (рисунок 163), поэтому необходимо использовать функционал федерации внешних баз данных пользователей Keycloak для взаимодействия со службами каталогов.

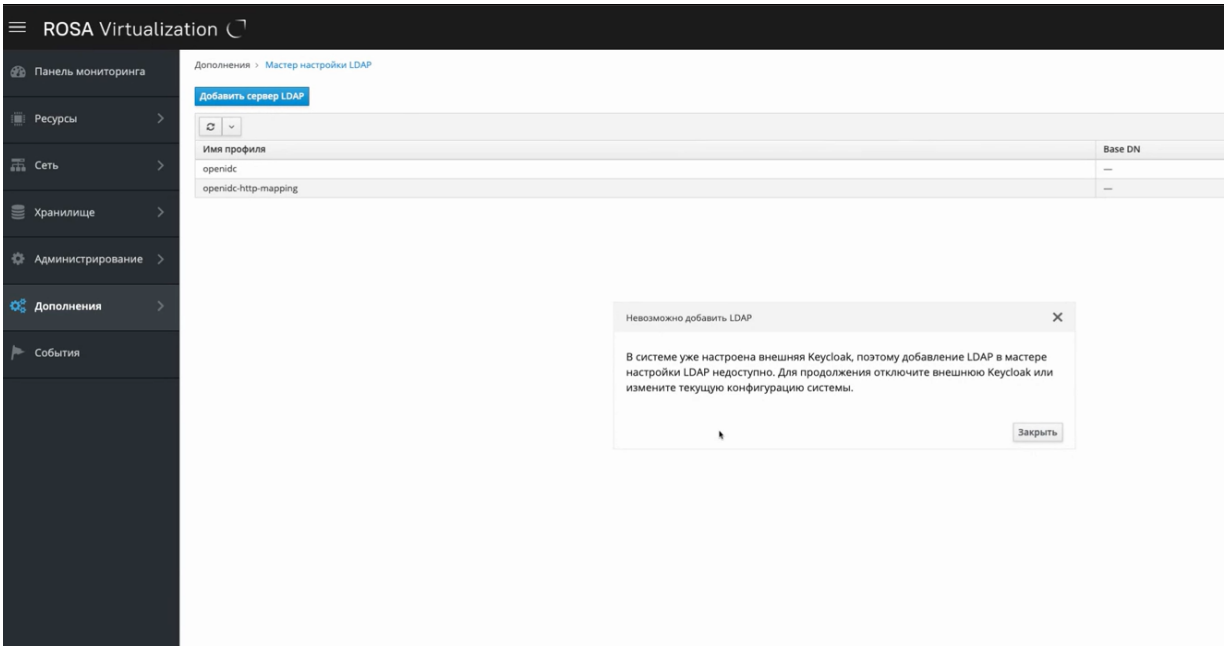

Рисунок 163 –Ограничение работы с LDAP

4.3.1 Управление пользователями в Keycloak

4.3.1.1 Группы

Группы в Keycloak управляют общим набором атрибутов для каждого пользователя. Пользователи могут быть членами любого количества групп и наследовать атрибуты, назначенные каждой группе.

Группы являются иерархическими. Группа может иметь несколько подгрупп, но у группы может быть только один родитель.

Управление группами осуществляется в разделе "Groups".

На странице в списке отображаются только группы верхнего уровня. Для просмотра и выполнения операций с дочерними группами, нужно выделить родительскую группу и открыть вкладку "Child groups". В дополнительном меню (вертикальное многоточие) дочерних групп доступны те же операции, что и в дополнительном меню родительских.

Для создания новой группы в разделе "Groups" необходимо нажать `New`, и ввести наименование группы (рисунок 164). Ввод подтвердить нажатием кнопки `Save`.

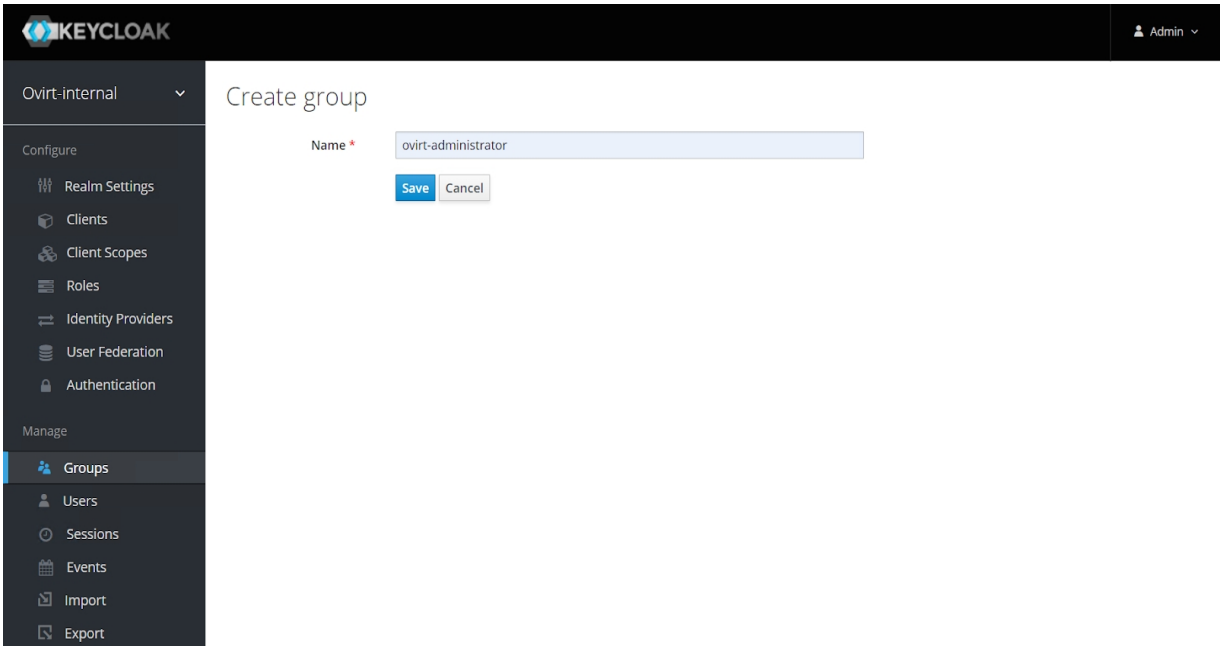

Рисунок 164 –Создать группу

4.3.1.2 Пользователи

Управление пользователями в Keycloak производится в разделе "Users" (рисунок 165).

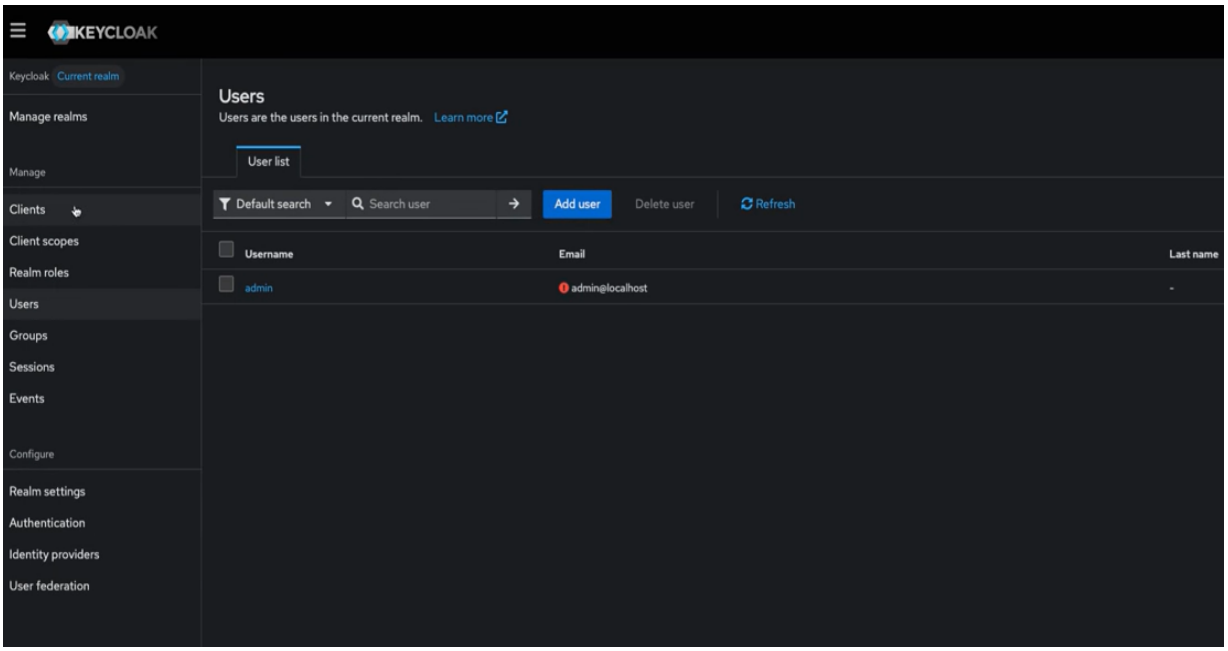

Рисунок 165 –Пользователи в Keycloak

Для создания учетной записи пользователя необходимо нажать `Add user`.

В оснастке добавления пользователя указать необходимые параметры (рисунок 166):

– Required user actions — (опционально) необходимые действия пользователя при входе в систему;
– Username — (обязательно) имя пользователя, используемое для аутентификации (логин);
– Email — (опционально) адрес электронной почты пользователя;
– Email verified — (опционально) при включении опции "Email verified" пользователю на указанный email придет письмо с инструкцией по активации аккаунта;
– First name — (опционально) имя пользователя;
– Last name — (опционально) фамилия пользователя;
– Groups — (опционально) при нажатии на `Join Groups` позволяет добавить пользователя в группы.

Ввод подтвердить нажатием кнопки `Save`.

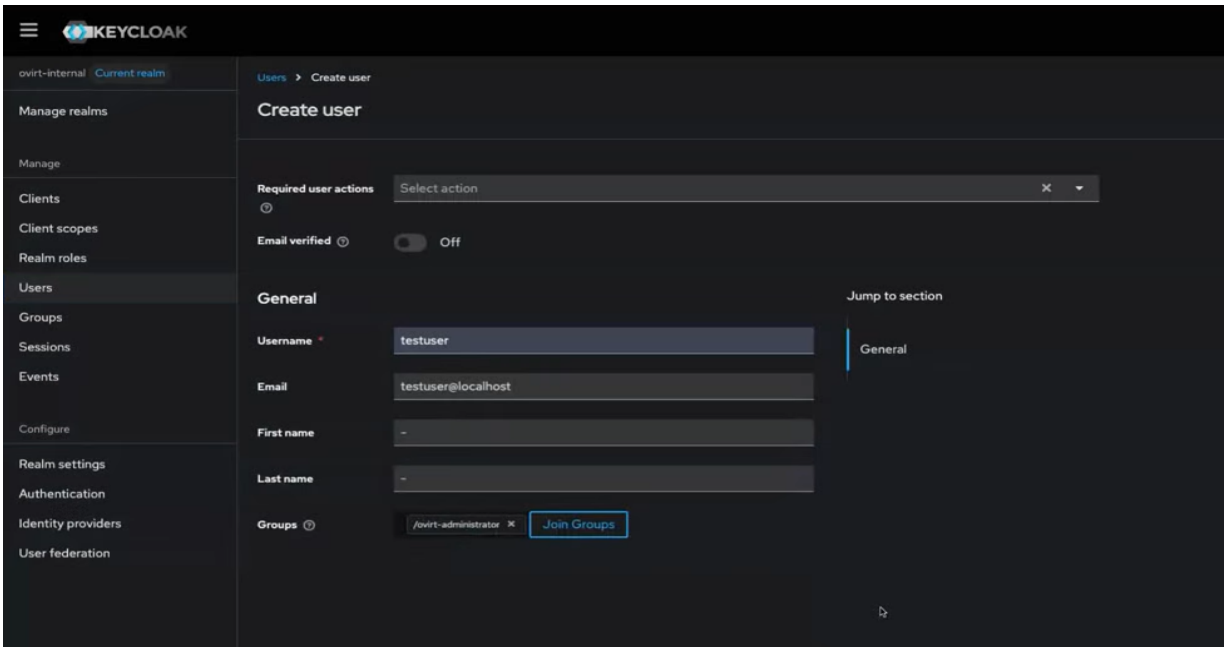

Рисунок 166 –Создать пользователя

Во вкладке "Users/Credentials" задать пользователю пароль нажатием кнопки `Set password`. Включенный переключатель Temporary указывает, что при первом входе пользователю необходимо будет изменить пароль (рисунок 167). Ввод подтвердить нажатием кнопки `Save`.

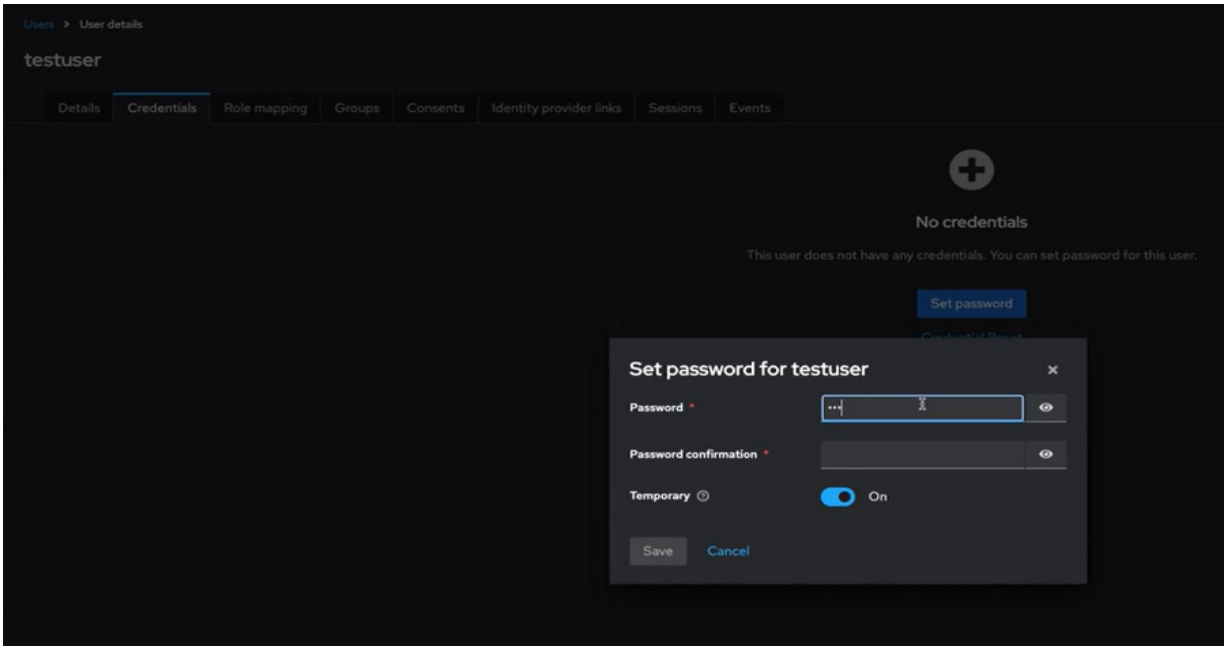

Рисунок 167 –Установка пароля пользователя в Keycloak

4.3.2 Импорт пользователей и групп в СУСВ

После создания пользователей и групп в Keycloak их нужно импортировать в СУСВ и назначить им роли. Возможны два способа импорта:

– Автоимпорт. Эта функция запускается при авторизации пользователей на Портале администрирования. При этом для успешного автоимпорта должны быть соблюдены следующие условия:

– Пользователь должен быть добавлен в группу, которая уже есть в СУСВ. По умолчанию, такой группой является группа ovirt-administrator;

– Импортированной группе должна быть назначена какая-либо административная или пользовательская роль. Например, группе ovirt-administrator назначена роль SuperUser;

– Пользователь должен успешно авторизоваться на Портале администрирования в соответствии с ролью группы.

– Ручной импорт. Требует вмешательства администратора для импорта пользователей и групп из Keycloak в СУСВ. Порядок действий для выполнения этой операции:

1) Идентифицироваться на портале администрирования с учетной записью, имеющей достаточные права для управления пользователями (по умолчанию admin@ovirt).

2) Перейти в раздел "Администрирование/Пользователи" (рисунок 168).

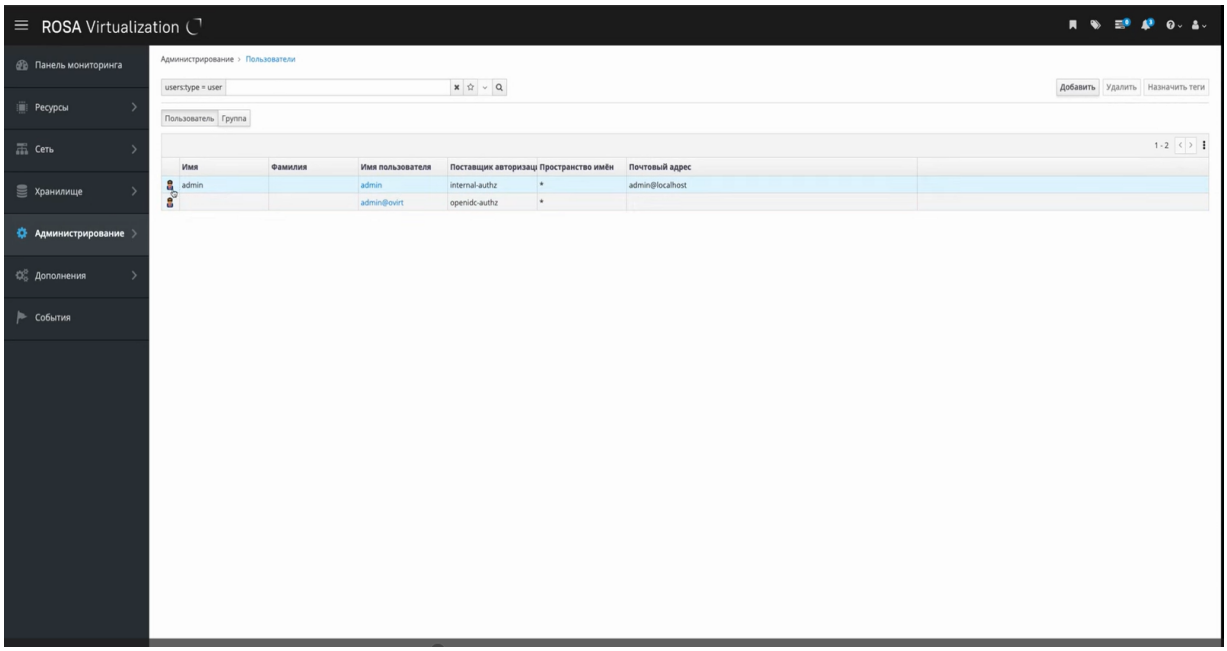

Рисунок 168 – Раздел Пользователи в СУСВ

3) Нажать кнопку Добавить.
4) В открывшейся оснастке (рисунок 169):

– Если необходимо импортировать пользователей:

– Убедиться, что активна опция Пользователь;
– Выбрать поиск в openidchttp (openidc-authz);
– Нажать Поиск;
– Отметить нужных пользователей и нажать Добавить или Добавить и закрыть.

– Если необходимо импортировать группы:

– Убедиться, что активна опция "Группа";
– Выбрать поиск в openidchttp (openidc-authz);
– Нажать Поиск;
– Отметить нужные группы и нажать Добавить или Добавить и закрыть.

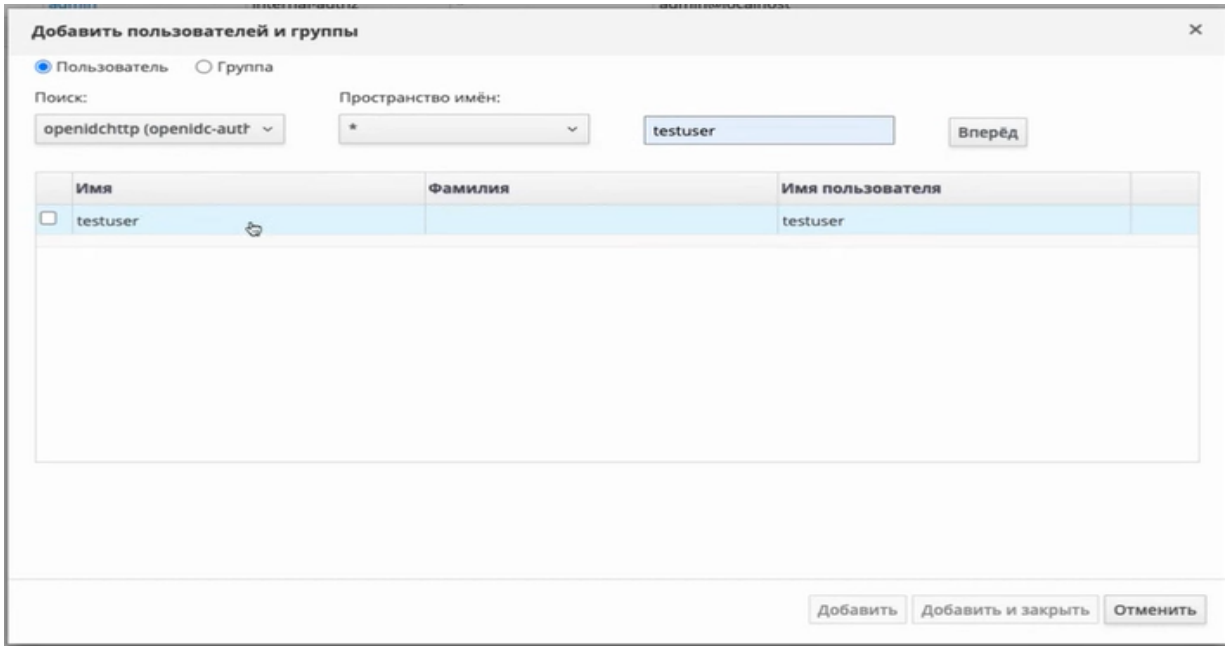

Рисунок 169 – Импорт Пользователя в СУСВ

Назначить импортированным пользователям/группам необходимые роли администратора или пользователя ресурсов, в соответствии с документом "РОСА Виртуализация 4. Руководство администратора. Часть 3. Эксплуатация".

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