Утвержден

НЦСВ.10001-01-УД

«VMMANAGER 6»

Руководство администратора

НЦСВ.10001-01 32 01

Листов 106

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

2025

АННОТАЦИЯ

Настоящий документ содержит руководства администраторов программного изделия «VMmanager 6» НЦСВ.10001-01 (далее — VMmanager), предназначенного для управления ВМ в едином интерфейсе. Создание среды виртуализации обеспечивается средствами «Операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (далее по тексту — Astra Linux).

В соответствии с «Требования по безопасности информации к средствам виртуализации» (утверждены приказом ФСТЭК России от 27.10.2022 г. № 187) под администраторами подразумеваются следующие роли пользователей: администратор безопасности средства виртуализации, администратор средства виртуализации, администратор ВМ.

В подразделе «Общие сведения о программе» указаны назначение и функции программы и сведения о технических и программных средствах, обеспечивающих выполнение данной программы.

В подразделе «Структура программы» приведены сведения о структуре программы, ее составных частях.

В подразделе «Описание реализации функций безопасности» приведено описание реализуемых в соответствии с «Требования по безопасности информации к средствам виртуализации» (утверждены приказом ФСТЭК России от 27.10.2022 г. № 187) функций.

В подразделе «Настройка программы» приведено описание действий по настройке программы на условия конкретного применения, в том числе настройки функций безопасности.

В подразделе «Проверка программы» приведено описание способов проверки, позволяющих дать общее заключение о работоспособности программы.

В подразделе «Сообщения системному программисту» указаны тексты сообщений, выводимых в ходе выполнения настройки, проверки программы, а также в ходе выполнения программы, описание их содержания и действий, которые необходимо предпринять по этим сообщениям.

В подразделе «Обеспечение безопасности» приведены сведения о порядке приемки программы, ее безопасной установке и настройке, реализации функций безопасности среды функционирования.

Оформление данного документа произведено по требованиям ГОСТ 19.503-79 «Руководство системного программиста. Требования к содержанию и оформлению».

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Полное наименование изделия: «VMmanager 6».

1.2. Обозначение изделия: НЦСВ.10001-01.

1.3. Разработчик и производитель изделия: АО «Экзософт».

Адрес нахождения: 121205, г. Москва, б-р Большой (Сколково Инновационного Центра), д. 42, стр. 1, эт. 0, пом. 150, раб. 14, тел. +7 (800) 775-47-78.

Адрес осуществления лицензируемого вида деятельности: 117105, г. Москва, Варшавское ш., д. 26.

1.4. Контрольные суммы установочного диска изделия приведены в «VMmanager 6». Формуляр» НЦСВ.10001-01 30 01.

1.5. Изделие обеспечивает решение функциональных задач по управлению ВМ в едином интерфейсе.

1.6. Изделие предоставляет следующие основные функциональные возможности:

- создание ВМ из собственного образа или по определенной конфигурации;
- управление ВМ через интерфейс администратора и портал самообслуживания;
- автоматическую подготовку узлов для ВМ с различными сетевыми конфигурациями;
- объединение узлов для ВМ в отказоустойчивые кластеры;
- управление адресным пространством;
- управление образами гостевых ОС;
- проведение мониторинга состояния узлов кластера и ВМ.

1.7. Для обеспечения безопасности при решении функциональных задач программное изделие совместно с Astra Linux предоставляет следующие основные функциональные возможности безопасности:

- доверенную загрузку ВМ;
- контроль целостности;
- резервное копирование;
- ограничение программной среды;
- защиту памяти;
- идентификацию и аутентификацию пользователей;
- управление доступом;
- управление потоками информации;
- регистрацию событий безопасности;
- централизованное управление (администрирование) ВМ и взаимодействие

между ними.

1.8. VMmanager работает под управлением Astra Linux.

1.9. В качестве аппаратного обеспечения VMmanager используются:

– сервер платформы (мастер-сервер), выполняющий функции по управлению виртуальными и сетевыми ресурсами;

– серверы узлов виртуализации, реализованные средствами qemu-kvm и libvirt из состава Astra Linux и управляемые мастер-сервером.

1.10. В качестве аппаратного обеспечения сервера платформы VMmanager используются средства вычислительной техники с процессорной архитектурой x86_64 (Intel и AMD) и набором инструкций SSE4.2. Минимальные и рекомендуемые требования (в зависимости от количества создаваемых ВМ) представлены в таблице 1. Поддерживаемые технологии дисков сервера — SSD, NVMe.

Таблица 1 — Минимальные и рекомендуемые требования к серверу платформы

	До 1500 ВМ		От 1500 до 3000 ВМ		От 3000 до 15000 ВМ		От 15000 до 22000 ВМ
	Мини-мальные	Реко-мендуе-мые	Мини-мальные	Рекомен-дуемые	Минималь-ные	Рекомен-дуемые	Минималь-ные
Процессор	2 ГГц	3 ГГц	2 ГГц	3 ГГц	2 ГГц	3 ГГц	3 ГГц
Количество ядер	2 шт.	4 шт.	4 шт.	8 шт.	16 шт.	16 шт.	16 шт.
Оперативная память	4 ГБ	8 ГБ	8 ГБ	16 ГБ	32 ГБ	64 ГБ	64 ГБ
Дисковое пространство (корневой раздел диска)	150 ГБ	300 ГБ	300 ГБ	600 ГБ	1 ТБ	2 ТБ	2 ТБ

В качестве аппаратного обеспечения сервера узла виртуализации используются средства вычислительной техники с процессорной архитектурой x86_64 (Intel и AMD). Минимальные и рекомендуемые требования представлены в таблице 2.

Таблица 2 — Минимальные и рекомендуемые требования к узлам виртуализации

	Минимальные	Рекомендуемые
Процессор	2.4 ГГц	3 ГГц
Количество ядер	4 шт.	8 шт.
Оперативная память	8 Гб	16 Гб
Дисковое пространство	1 ТБ	2 ТБ

1.11. Изделие предназначено для обработки информации, не содержащей сведения, составляющие государственную тайну, и может быть применено:

– в государственных информационных системах до первого класса защищенности включительно[1)];

– в информационных системах персональных данных до первого уровня защищенности включительно[2)];

– в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды до первого класса защищенности включительно[3)];

– в составе значимых объектов критической информационной инфраструктуры до первой категории включительно[4)];

– в информационных системах общего пользования II класса[5)] и иных информационных (автоматизированных) системах при выполнении указаний по эксплуатации, приведенных в разделе 6 «VMmanager 6». Технические условия» НЦСВ.10001-01 90 01.

[1)]В соответствии с приказом ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

[2)]В соответствии с приказом ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

[3)]В соответствии с приказом ФСТЭК России от 14.03.2014 № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

[4)]В соответствии с приказом ФСТЭК России от 25.12.2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

[5)]В соответствии с приказом от 31.08.2010 ФСБ России № 416 и ФСТЭК России № 489 «Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования».

2. ОСНОВНАЯ ЧАСТЬ

2.1. Общие сведения о программе

ПО VMmanager предназначено для управления средой виртуализации, создание которой обеспечивается средствами Astra Linux. В основные возможности программы входит:

- создание ВМ из собственного образа или по определенной конфигурации;
- управление ВМ через интерфейс администратора и портал самообслуживания;
- автоматическая подготовка узлов для ВМ с различными сетевыми конфигурациями;
- объединение узлов для ВМ в отказоустойчивые кластеры;
- управление адресным пространством;
- управление образами гостевых ОС;
- проведение мониторинга состояния узлов кластера и ВМ.

2.2. Структура программы

2.2.1. Подсистемы, реализующие функции безопасности средства

К подсистемам, реализующим функции безопасности, относятся:

- подсистема идентификации и аутентификации пользователей;
- подсистема управления доступом;
- подсистема управления потоками информации;
- подсистема резервного копирования;
- подсистема централизованного управления (администрирования) ВМ и взаимодействия между ними;
- подсистема контроля целостности;
- подсистема регистрации событий;
- подсистема защиты памяти.

Подсистема идентификации и аутентификации пользователей выполняет следующие функции:

- синхронизация с LDAP;
- настройка политик безопасности;
- авторизация пользователей.

Подсистема управления доступом выполняет следующие функции:

- управление пользователями;

– управление группами пользователей.

Подсистема управления потоками информации выполняет следующие функции:

– настройка сети в кластере;
– настройка сети узла;
– настройка сетевого взаимодействия ВМ.

Подсистема резервного копирования выполняет следующие функции:

– управление резервными копиями;
– выполнение резервного копирования по расписанию;
– управление хранилищами;
– резервное копирование платформы.

Подсистема централизованного управления ВМ выполняет следующие функции:

– управление ВМ;
– создание и настройка ВМ;
– управление образами ВМ;
– настройка ОС;
– настройка пользовательских образов;
– настройка конфигурации ВМ;
– управление репозиториями.

Подсистема контроля целостности выполняет следующие функции:

– доверенная загрузка ВМ;
– контроль целостности;
– ограничение программной среды.

Подсистема регистрации событий выполняет функцию регистрации событий безопасности.

Подсистема защиты памяти выполняет функцию защиты памяти.

2.2.2. Подсистемы, поддерживающие выполнение функций безопасности

К подсистемам, поддерживающим выполнение функций безопасности, относятся:

– подсистема управления личным кабинетом;
– подсистема управления сетевыми подключениями;
– подсистема управления кластерами;
– подсистема управления узлами кластера;
– подсистема настройки скриптов и переменных;
– подсистема настройки ВМ;
– подсистема статистики;
– подсистема проверки авторизации пользователя;

– подсистема лицензирования.

Подсистема управления личным кабинетом выполняет следующие функции:

– настройка профиля пользователя;
– настройка SSH-соединения.

Подсистема управления сетевыми подключениями выполняет следующие функции:

– управление физическими сетями;
– управление пулами IP-адресов;
– управление IP-адресами;
– управление DNSBL;
– настройка прокси.

Подсистема управления кластерами выполняет следующие функции:

– управление кластерами;
– настройка карточки кластера;
– настройка отказоустойчивости;
– настройка локальных хранилищ кластера;
– настройка сетевых хранилищ кластера.

Подсистема управления узлами кластера выполняет следующие функции:

– управление узлами;
– мониторинг сведений об узлах;
– настройка распределения ВМ;
– отслеживание статистики;
– управление дисковым пространством.

Подсистема настройки скриптов и переменных выполняет следующие функции:

– настройка скриптов для ВМ;
– настройка скриптов для узлов;
– настройка скриптов;
– настройка переменных.

Подсистема настройки ВМ выполняет следующие функции:

– миграция;
– переустановка ОС;
– настройка дисков;
– настройка SPICE;
– настройка VNC;
– снимки ВМ;

– статистика.

Подсистема статистики выполняет следующие функции:

– сбор статистики;

– визуализация данных.

Подсистема проверки авторизации пользователя выполняет функцию авторизации пользователя.

Подсистема лицензирования выполняет функцию активации и проверки валидности лицензии.

2.2.3. Подсистемы, не влияющие на выполнение функций безопасности

К подсистемам, не влияющим на выполнение функций безопасности, относятся:

– подсистема установки;

– подсистема настройки сервисов;

– подсистема пользовательских уведомлений;

– подсистема системного интерфейса;

– подсистема регистрации сервисов;

– подсистема управления межсервисным взаимодействием;

– подсистема мониторига (сбора метрик использования платформы).

Подсистема установки выполняет следующие функции:

– установка платформы;

– проверка лицензирования;

– настройка обновлений;

– управление платформой;

– настройка виджетов кластеров;

– настройка виджетов задач;

– настройка виджетов узлов;

– настройка виджетов мониторинга.

Подсистема настройки сервисов выполняет следующие функции:

– обзор системы;

– настройки почты;

– клиентский сервис;

– интеграция с сервисами;

– обеспечение миграции;

– настройка статистики.

Подсистема пользовательских уведомлений выполняет следующие функции:

– настройка центра уведомлений;

– настройка мессенджеров.

Подсистема системного интерфейса выполняет следующие функции:

– сортировка;

– навигация;

– настройка действий;

– управление задачами.

Подсистема регистрации сервисов выполняет функцию регистрации внутренних сервисов в consul.

Подсистема управления межсервисным взаимодействием выполняет функцию маршрутизации запросов к платформе.

Подсистема мониторинга (сбора метрик использования платформы) выполняет следующие функции:

– мониторинг состояния узлов;

– мониторинг состояния ВМ.

2.3. Описание реализации функций безопасности

2.3.1. Доверенная загрузка ВМ

Для осуществления доверенной загрузки ВМ в VMmanager используются средства Astra Linux («Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1» РУСБ.10015-01 97 01-1). В целях блокировки запуска ВМ при выявлении нарушения целостности конфигурации виртуального оборудования данной ВМ или нарушения целостности файлов виртуальной базовой системы ввода-вывода применяется механизм контроля целостности «отпечаток конфигурации».

Для включения доверенной загрузки ВМ необходимо выполнить следующие действия на узле виртуализации VMmanager:

1) установить пакет ПО astra-kvm-secure;

2) установить следующие настройки в конфигурационном файле `/etc/libvirt/libvirtd.conf`:

   – `integrity_control = 1`;

   – `file_integrity_on_startup_VM = 1`;

3) перезапустить сервис libvirt командой: `sudo systemctl restart libvirtd`

2.3.2. Контроль целостности

Для осуществления контроля целостности в VMmanager используются следующие

механизмы, реализованные в Astra Linux (РУСБ.10015-01 97 01-1):

– механизм контроля запуска исполняемых файлов формата ELF и контроля расширенных атрибутов в ЗПС;

– механизм регламентного контроля целостности Another File Integrity Checker (AFICK);

– механизм контроля целостности «отпечаток конфигурации»;

– механизм контроля целостности исполняемых файлов гостевой ОС;

– механизм контроля целостности областей памяти ВМ (по запросу из гостевой ОС).

Контроль целостности осуществляется для следующих типов объектов: конфигурации виртуального оборудования ВМ, конфигураций объектов виртуальной инфраструктуры, исполняемых файлов и параметров настройки средств виртуализации, файлов виртуальной базовой системы ввода-вывода (первичного загрузчика ВМ), исполняемых файлов гостевой ОС ВМ, областей памяти ВМ.

Для включения контроля целостности необходимо выполнить следующие действия на узле виртуализации VMmanager:

1) установить следующие настройки в конфигурационном файле `/etc/digsig/digsig_initramfs.conf`:

```
DIGSIG_XATTR_MODE = 1;
```

2) выполнить команду:

```
update-initramfs -u -k all
```

3) перезагрузить узел виртуализации.

Проверка целостности с использованием средств динамического контроля целостности производится непосредственно в момент обращения (попытки чтения) к объектам контроля. Это обращение производится средством libvirt только в процессе его загрузки.

2.3.3. Резервное копирование

Для осуществления резервного копирования в VMmanager используются средства Astra Linux (РУСБ.10015-01 97 01-1). Резервное копирование образов ВМ и конфигурации виртуального оборудования ВМ, а также сведений о событиях безопасности реализуется с использованием встроенных в средства виртуализации ОС механизмов резервного копирования (инструментов командной строки `virsh backup-begin`, `virsh dumpxml` и `virsh snapshot-create`), а также встроенных в ОС средств резервного копирования.

ПО резервного копирования и восстановления из состава ОС включает

инструменты командной строки и распределенные системы управления хранилищами данных:

- комплекс программ Bacula;
- инструмент копирования rsync;
- инструменты архивирования и копирования tar, cpio, gzip, cp.

Для подготовки окружения узла виртуализации VMmanager к резервному копированию образов ВМ и конфигурации виртуального оборудования ВМ необходимо выполнить следующие действия:

1) скопировать shell-скрипты для работы с резервными копиями из директории `/scripts` на сервере платформы в директорию на узле виртуализации;
2) указать значения переменных в файле shell-скрипта `vars.sh`:
   - VM_URL — URL сервера платформы;
   - VM_LOGIN — email учетной записи администратора;
   - VM_PASS — пароль учетной записи администратора;
   - VM_IP — IP-адрес сервера платформы;
   - BACKUP_LOCATION — директория хранения резервных копий.

Для создания резервной копии ВМ требуется запустить на узле виртуализации VMmanager скрипт `backup.sh` командой:

```
./backup.sh <id BM>
```

Скрипт запускает процесс создания резервной копии средствами VMmanager. Архив с резервной копией будет сохранен в поддиректорию внутри директории, указанной в параметре `BACKUP_LOCATION` в файле `vars.sh`.

Для восстановления ВМ из резервной копии требуется запустить на узле виртуализации VMmanager скрипт `restore.sh` командой:

```
./restore.sh <имя директории с резервной копией>
```

Логика работы скрипта:

1) если восстанавливаемая ВМ существует в VMmanager, скрипт проверяет существует ли указанная резервная копия в VMmanager. Если есть, запускает восстановление средствами VMmanager. Если нет, запускает восстановление из директории хранения резервных копий;
2) если восстанавливаемая ВМ отсутствует в VMmanager, предложит администратору создать ее средствами VMmanager. При создании будет проведена проверка основного IP-адреса ВМ. Если адрес занят, предложит администратору занять новый IP-адрес. После создания ВМ скрипт добавит сохраненную резервную копию в VMmanager и запустит восстановление.

Резервное копирование параметров настройки средств виртуализации в VMmanager реализовано через механизм резервного копирования платформы, описанного в 2.4.3.6 данного документа.

Для резервного копирования сведений о событиях безопасности необходимо выполнить следующие действия:

1) запустить программу «Настройка регистрации системных событий — Модуль настройки системы» командой:

```
sudo fly-admin-events
```

2) перейти в меню «Настройки — Ротация основного лога» и установить значение «Максимальный размер файла» меньшее, чем текущий размер лога. Например: «1 МБ», **[Сохранить]**, **[Да]**;

3) выполнить попытку ротации лога вне регламента, установленного в планировщик cron, командой:

```
sudo logrotate /etc/logrotate.d/syslog-ng-mod-astra
```

4) убедиться, что ротация совершилась в связи с выполнением условий ротации об ограничении области памяти, отведенной под журнал событий.

Проверить наличие архива командой:

```
ls -la /parsec/log/astra/events
```

После запуска утилиты должен быть создан архивный журнал `events.1`, новый журнал очищен, а также должна присутствовать запись о ротации.

2.3.4. Ограничение программной среды

Для осуществления ограничений программной среды в VMmanager используются средства Astra Linux (РУСБ.10015-01 97 01-1).

Контроль за запуском компонентов ПО, обеспечивающий выявление и блокировку запуска компонентов ПО, не включенных в перечень (список) компонентов, разрешенных для запуска, осуществляется штатными средствами ОС:

1) механизмом динамического контроля целостности (режим ЗПС) исполняемых файлов и разделяемых библиотек формата ELF при запуске программы на выполнение;

2) применением режима Киоск-2, который служит для ограничения прав пользователей на запуск программ в ОС. Степень этих ограничений задается маской киоска, которая накладывается на права доступа к исполняемым файлам при любой попытке пользователя получить доступ.

Выявление и блокировка запуска компонентов ПО, целостность которого нарушена, осуществляется механизмом динамического контроля целостности

исполняемых файлов и разделяемых библиотек формата ELF путем внедрения цифровой подписи в файлы, входящие в состав ПО. При включенном режиме контроля цифровой подписи выполняться будут только подписанные исполняемые файлы.

Для включения контроля целостности необходимо выполнить следующие действия на узле виртуализации VMmanager:

1) установить следующие настройки в конфигурационном файле `/etc/digsig/digsig_initramfs.conf`:

- `DIGSIG_XATTR_MODE = 1`;
- `DIGSIG_ELF_MODE = 1`.

2) выполнить команду:

```
update-initramfs -u -k all
```

3) перезагрузить узел виртуализации.

2.3.5. Защита памяти

Для очистки остаточной информации в памяти VMmanager использует механизмы, реализованные в Astra Linux. Указанные механизмы обеспечивают очищение неиспользуемых блоков файловой системы непосредственно при их освобождении (распределении) и очищение активных разделов страничного обмена. Описание механизмов очистки освобождаемой внешней памяти приведено в документе РУСБ.10015-01 97 01-1. Дополнительная настройка VMmanager не требуется.

Защита задач ядра и процессов пользователей при доступе к страницам оперативной памяти обеспечивается архитектурой и параметрами ядра Astra Linux. Для предупреждения несанкционированных изменений модулей ядра в составе Astra Linux применяется модуль lkrg, который обеспечивает мониторинг угроз и блокирование несанкционированных изменений в ядре Astra Linux. Таким образом, целостность всей области памяти ВМ при использовании lkrg обеспечивается по умолчанию. Для обработки критически важных данных рекомендуется на сервере виртуализации использовать Astra Linux с включенным модулем lkrg и ЗПС, а в ВМ применять Astra Linux на усиленном или максимальном уровне защищенности с ядром hardened и включенным ЗПС.

Для включения модуля lkrg необходимо на каждом компьютере, выполняющем функцию узла виртуализации, выполнить следующие действия:

1) установить пакет `lkrg-<версия_ядра>`. При использовании ядра linux-6.6-generic команда для установки имеет следующий вид:

```
sudo apt install lkrg-6.6
```

2) перезагрузить компьютер;

3) включить использование модуля lkrg командой:

```
sudo astra-lkrg-control enable
```

Для изоляции и управления виртуальными гостевыми машинами используется технология KVM, которая включает специальный модуль ядра KVM и средство создания виртуального аппаратного окружения QEMU для изоляции и управления виртуальными гостевыми машинами. KVM, используя загруженный в память модуль ядра, с помощью драйвера пользовательского режима эмулирует слой аппаратного обеспечения, в среде которого могут создаваться и запускаться ВМ.

Более подробно механизмы защита памяти в среде виртуализации, реализованные в Astra Linux, описаны в документе РУСБ.10015-01 97 01-1.

2.3.6. Идентификация и аутентификация пользователей

Идентификация и аутентификация пользователей в VMmanager выполняется с учетом требований ГОСТ Р 58833-2020 «Защита информации. Идентификация и аутентификация. Общие положения».

Вход в программу осуществляется по идентификатору (email) и паролю. Защита пароля пользователя обеспечивается при его вводе за счет отображения вводимых символов условными знаками. При входе в программу осуществляется идентификация и проверка подлинности субъектов доступа процедурой аутентификации, реализованной средствами VMmanager.

При попытке ввода неправильного значения идентификатора или пароля пользователя в интерфейсе VMmanager выводится сообщение о том, что вход в систему не выполнен, и пользователю предлагается ввести правильный идентификатор и пароль еще раз.

Установка пароля пользователя для первичной аутентификации, возможность смены установленного администратором средства виртуализации пароля пользователя после его первичной аутентификации, невозможность установления одинаковых идентификаторов и паролей для разных пользователей, хранение аутентификационной информации пользователя средства виртуализации в защищенном формате или в защищенном хранилище, требования к минимальной длине пароля (не менее восьми символов при алфавите пароля не менее 70 символов) реализованы с помощью службы FreeIPA, входящей в состав Astra Linux. Порядок синхронизации со службой FreeIPA описан в 2.4.4.3 данного документа.

Ограничение количества неуспешных попыток входа и блокирования учетной записи и сеанса доступа пользователя при превышении числа неуспешных попыток аутентификации в системе устанавливается администратором с помощью настроек ограничения аутентификации, описанными в 2.4.4.4 данного документа.

Блокировка учетных записей пользователей совершается автоматически по заданному параметру количества следующих подряд неудачных попыток аутентификации пользователя. Разблокировка учетной записи пользователя производится автоматически в соответствии с настройками ограничения аутентификации, описанными в 2.4.4.4 данного документа.

Взаимная идентификация и аутентификация пользователей и средства виртуализации при удаленном доступе осуществляется с использованием удаленной SSH-аутентификации, а также с использованием сетевого протокола сквозной доверенной аутентификации в ЕПП (удаленная SASL-аутентификация с поддержкой Kerberos).

2.3.7. Управление доступом

Доступ в платформу осуществляется по протоколу HTTPS с использованием шифрования TLS. Работа с программой возможна только после прохождения обязательной процедуры аутентификации.

Доступ к узлам кластера осуществляется по протоколам SSH с использованием шифрования и ПО qemu-tls.

В программе реализован механизм ролевого управлениям доступом. Ролевое управление доступом обеспечивает разграничение возможностей выполнения привилегированных операций со средствами виртуализации.

Реализация ролевого метода управления доступом подразумевает разграничение доступа по ролям:

- учетная запись уровня «Пользователь» — соответствует роли администратора ВМ, определяемой требованиями ФСТЭК России;
- учетная запись уровня «Продвинутый пользователь» — соответствует роли разработчика ВМ, определяемой требованиями ФСТЭК России;
- учетная запись уровня «Администратор» — соответствует роли администратора средства виртуализации, определяемой требованиями ФСТЭК России;
- администратор безопасности средства виртуализации (функции реализованы средствами Astra Linux).

2.3.8. Управление потоками информации

Управление потоками информации между ВМ и информационными (автоматизированными) системами на канальном и сетевом уровнях, а также контроль взаимодействия ВМ между собой реализуется средствами подсистемы nftables, входящей

в состав Astra Linux.

Настройка подсистемы nftables на узле виртуализации VMmanager осуществляется с помощью скрипта настройки. Для настройки nftables требуется скопировать скрипт из директории `/scripts` на сервере платформы на узел виртуализации.

Возможные действия по работе со скриптом настройки nftables:

– просмотреть список правил nftables для ВМ — запустить скрипт командой:

```
./firewall.sh <имя ВМ> list
```

Чтобы определить имя ВМ, необходимо выполнить команду:

```
virsh list
```

– удалить правило из списка — запустить скрипт командой:

```
./firewall.sh <имя ВМ> remove <handle-номер правила>
```

Чтобы определить имя ВМ, необходимо выполнить команду:

```
virsh list
```

Handle-номера правил отображаются при просмотре списка правил nftables;

– добавить правило для входящего трафика — запустить скрипт командой:

```
./firewall.sh <имя ВМ> add --direction in [--ports <порты>] [--
ip <IP-адреса>]
```

Чтобы определить имя ВМ, необходимо выполнить команду:

```
virsh list
```

Скрипт добавит правило, запрещающее подключение к ВМ с указанных IP-адресов на указанные порты;

– добавить правило для исходящего трафика — запустить скрипт командой:

```
./firewall.sh <имя ВМ> add --direction out [--ports <порты>] [--
ip <IP-адреса>].
```

Чтобы определить имя ВМ, необходимо выполнить команду:

```
virsh list
```

Скрипт добавит правило, запрещающее подключение с ВМ на указанные порты указанного IP-адреса. Если при добавлении правила не указаны IP-адреса и/или порты, правило применится для всех IP-адресов и/или портов.

2.3.9. Регистрация событий безопасности

Для регистрации событий безопасности в VMmanager используются следующие принципы:

1) регистрация событий безопасности в средстве виртуализации выполняется с учетом требований ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации»;

2) сбор, запись и хранение информации о событиях безопасности осуществляются с использованием расширенной подсистемы протоколирования Astra Linux, осуществляющей регистрацию событий с использованием сервиса auditd совместно с модулем фильтрации syslog-ng-mod-astra и демоном libvirtd путем ведения журналов аудита событий безопасности согласно заданным правилам. Состав регистрируемой информации соответствует ГОСТ Р 59548-2022;

3) регистрация событий безопасности, связанных с функционированием средства виртуализации, осуществляется в системные журналы `/var/log/`, `/var/log/audit/audit` и защищенный журнал `/parsec/log/astra/events`. Также регистрация событий осуществляется для каждой созданной ВМ. Журналы работы ВМ хранятся в директории `/var/log/libvirt/qemu/`. Настройка регистрации событий демона libvirtd осуществляется в файле `/etc/libvirt/libvirtd.conf`. Чтобы новая конфигурация загрузилась в память средства виртуализации, необходимо выполнять перезапуск libvirtd командой:

```
sudo systemctl restart libvirtd
```

4) просмотр и анализ событий безопасности осуществляется администратором с использованием консольных (ausearch, aureport, aulast и auvirt) и графических (ksystemlog и fly-event-viewer) инструментов Astra Linux. Утилита auvirt используется для поиска в журналах аудита записей, созданных libvirt, чтобы вывести список сеансов ВМ. Также утилита выполняет поиск таких событий, как остановка хост-системы, отказы в доступе, связанные с гостевыми системами, и аномальные события, связанные с QEMU-процессами;

5) оповещение администратора безопасности средства виртуализации о событиях безопасности осуществляется в регистрационные журналы;

6) информирование о событиях безопасности осуществляется с использованием модуля VMmanager «Центр уведомлений», работа с которым описана в 2.4.9 данного документа;

7) реакция на события безопасности задается с использованием программы «Настройка регистрации системных событий» (модуль «Настройки системы»),

входящей в состав Astra Linux, описание утилиты приведено в электронной справке;

8) определение перечня событий, необходимых для регистрации и учета для каждой функции безопасности, выполняется с использованием программы «Настройка регистрации системных событий» (модуль «Настройки системы»), входящей в состав Astra Linux, описание утилиты приведено в электронной справке;

9) в каждой записи журнала событий безопасности регистрируются номер (уникальный идентификатор) события, дата, время, тип события безопасности;

10) записи журнала событий безопасности представляются в структурированном виде и содержат время события безопасности, взятое из ОС;

11) целостность сведений о событиях безопасности реализуется совместными применением мандатного контроля целостности и атрибута доступа «`chattr +a`»:

- для файла журнала безопасности `/parsec/log/astra/events` установлен атрибут «`chattr +a`», который разрешает доступ к файлу только на чтение и на добавление в конец новых строк. Проверка установки атрибута выполняется с помощью команды:

  ```
  sudo pdp-ls -d -P /parsec/log/astra/events
  ```

  Удалить или изменить файл невозможно. Запрет распространяется на всех пользователей вне зависимости от их привилегий;
- файл журнала защищен от изменения средствами МКЦ (файл журнала, каталог и ведущий его процесс syslog-ng-mod-astra имеют высокую метку целостности);
- удаление журнала событий контролируется событием «Журнал событий удален»;
- переименование или перемещение журнала событий контролируется событием «Журнал событий переименован или перемещен»;
- ротация журнала событий контролируется событием «Журнал событий ротирован»;
- прочие манипуляции с журналом событий контролируются событием «Журнал событий изменен недоверенным процессом», за исключением процессов syslog-ng и logrotate;

12) просмотр событий безопасности при проверках осуществляется через команды:

– `sudo fly-event-viewer` — для журнала `/parsec/log/astra/events`;

– `sudo ksystemlog` — для системных журналов;

13) в каждой записи журналов событий безопасности регистрируется значение параметра критичности.

2.3.10. Централизованное управление (администрирование) ВМ и взаимодействие между ними

В VMmanager реализовано создание, модификация, хранение, получение и удаление (в т.ч. централизованное) образов ВМ в информационной (автоматизированной) системе.

Для централизованного хранения образов ВМ используются локальные и сетевые хранилища данных. Хранилище определяет физическое расположение файлов-образов и может быть различных типов. Хранилище должно быть доступно для подключения на серверах виртуализации. Поддерживаемые типы хранилищ и порядок их подключения указаны в 2.4.5.7 данного документа.

VMmanager поддерживает возможность миграции ВМ между узлами виртуализации. Миграция позволяет перенести работу ВМ с одного физического хоста (узла виртуализации) на другой. Существует два варианта миграции — с остановкой работы ВМ и без остановки работы (живая миграция). Управление перемещением ВМ реализуется с использованием интерфейсов управления средствам виртуализации libvirt в соответствии с установленными правилами сетевого взаимодействия. Инструкции по миграции ВМ приведены в 2.4.8.5 данного документа.

2.4. Настройка программы

2.4.1. Установка программы

VMmanager функционирует в среде Astra Linux (очередное обновление 1.8) на усиленном уровне защищенности (режим «Воронеж»).

Для обеспечения корректного функционирования VMmanager необходимо выполнить действия по безопасной установке и настройке средства, описанные в п.3.2.

Порядок установки:

1) отключить ЗПС;

2) подключиться к серверу платформы по SSH;

3) подключить ISO-образ платформы командой:

```
mount -o iso9660 <path_to_iso> /mnt
```

4) запустить скрипт установки командами:

```
cd /mnt/vmmanager6_master && sudo sh install.sh
```

5) дождаться окончания установки. Если установка завершилась успешно, то в терминале будет выведена ссылка для перехода в платформу и URL репозитория с образами ОС;

6) перейти в интерфейс платформы по полученной ссылке из п. 4 и ввести данные первого пользователя;

7) включить режим ЗПС командой:

```
astra-digsig-control enable
```

8) скачать открытый ключ разработчика изделия для ЗПС по ссылке: `https://download.ispsystem.com/6/astra_se/exo-soft_pub.key`

9) скопировать открытый ключ на сервер платформы в директорию `/etc/digsig/keys/`;

10) подключиться к серверу платформы по SSH;

11) инициализировать ключ для всех ядер центрального процессора командой:

```
update-initramfs -u -k all
```

12) перезагрузить сервер платформы.

2.4.2. Активация лицензии

При первичной активации лицензии необходимо:

1) в правом меню нажать значок шестеренки, перейти на вкладку «Обзор системы»;

2) в разделе «Активация лицензии» во вкладке «Активировать вручную» скачать «Ключ привязки»;

3) отправить ключ привязки, id и токен лицензии в техническую поддержку ISPsystem или отдел продаж дистрибьютора. В ответ будет получен файл лицензии;

4) в разделе «Активация лицензии» загрузить файл лицензии и нажать кнопку **[Активировать]**.

При повторной активации лицензии необходимо:

1) подключиться к серверу с платформой по SSH с правами суперпользователя (по умолчанию root);

2) удалить из директории `/opt/ispsystem/license/` все файлы, кроме `machine_id`:

```
find /opt/ispsystem/license/ -type f -not -name 'machine_id'
-delete
```

3) подождать несколько минут для генерации нового ключа привязки;

4) выполнить действия, необходимые при первичной активации.

За один месяц до окончания срока лицензии в интерфейсе появится баннер с напоминанием о продлении. Чтобы продлить лицензию, повторно выполните действия для активации лицензии.

2.4.3. Настройка платформы

2.4.3.1. Подключение SSL-сертификата

Для доступа к платформе по протоколу HTTPS необходимо подключить SSL-сертификат, созданный с использованием RSA-ключа. Порядок подключения:

1) нажать на значок «шестеренка» и перейти на вкладку «Глобальные настройки»;
2) нажать кнопку **[Переподключить сертификат]**;
   а) чтобы подключить выпущенный сертификат:
      - ввести произвольное название в поле «Имя SSL-сертификата»;
      - ввести содержимое открытого ключа SSL-сертификата в поле «SSL-сертификат»;
      - при наличии файла цепочки сертификатов, ввести содержимое файла в поле «Цепочка SSL-сертификатов»;
      - ввести содержимое приватного ключа SSL-сертификата в поле «Приватный ключ SSL-сертификата»;

   б) чтобы выпустить и подключить сертификат Let’s Encrypt:
      - перейти на вкладку «Let’s Encrypt»;
      - ввести домен, для которого нужно выпустить сертификат;
      - ввести e-mail администратора для получения уведомлений о статусе сертификата;
3) нажать кнопку **[Подключить сертификат]**.

Пример добавления сертификата приведен на рис. 1.

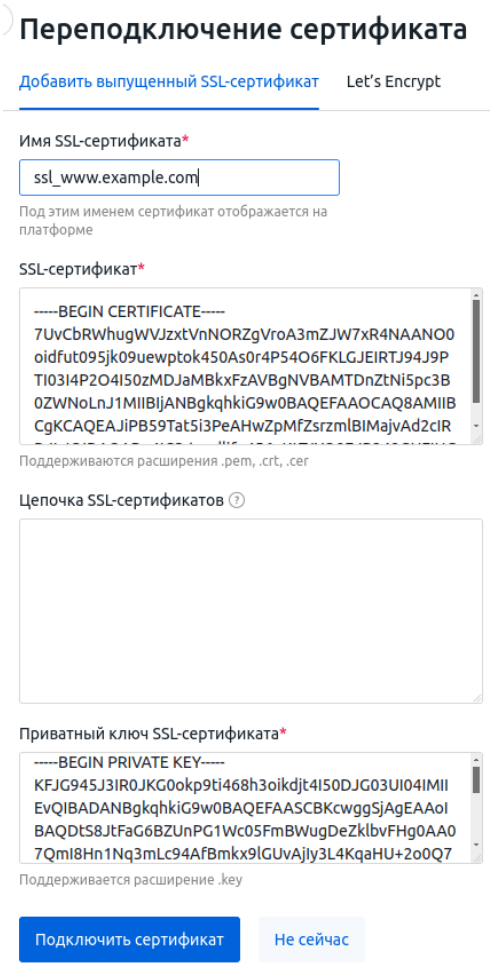

Рис. 1 — Добавление SSL-сертификата

2.4.3.2. Настройка почтового сервера

Почтовый сервер используется для отправки уведомлений о завершении долгосрочных операций и приглашений новым пользователям.

По умолчанию в платформе используется почтовый сервер ISPsystem. Порядок изменения настроек почтового сервера:

1) нажать на значок «шестеренка» и перейти на вкладку «Настройка почты»;
2) выбрать почтовый сервис:
   - «Своя почта» — собственный почтовый сервер;
   - «Яндекс.Почта»;
   - «Почта Mail.ru»;
   - «Gmail»;
3) для подключения собственного почтового сервера:
   - ввести домен или публичный адрес сервера исходящей почты;
   - ввести SMTP-порт;
   - для работы по протоколу SSL установить опцию «Использовать SSL»;
4) если почтовый сервер требует авторизацию:

– установить опцию «Авторизация на почтовом сервере»;

– ввести логин и пароль для отправки почты;

5) **при** необходимости отправлять пользователям информацию о доступах к ВМ по почте, включить опцию «Разрешить отправку письма с доступами к VM»;

6) в блоке «Тестовое письмо» ввести email и нажать кнопку **[Отправить тестовое письмо]**;

7) нажать кнопку **[Сохранить]**.

Пример настройки почтового сервера приведен на рис. 2.

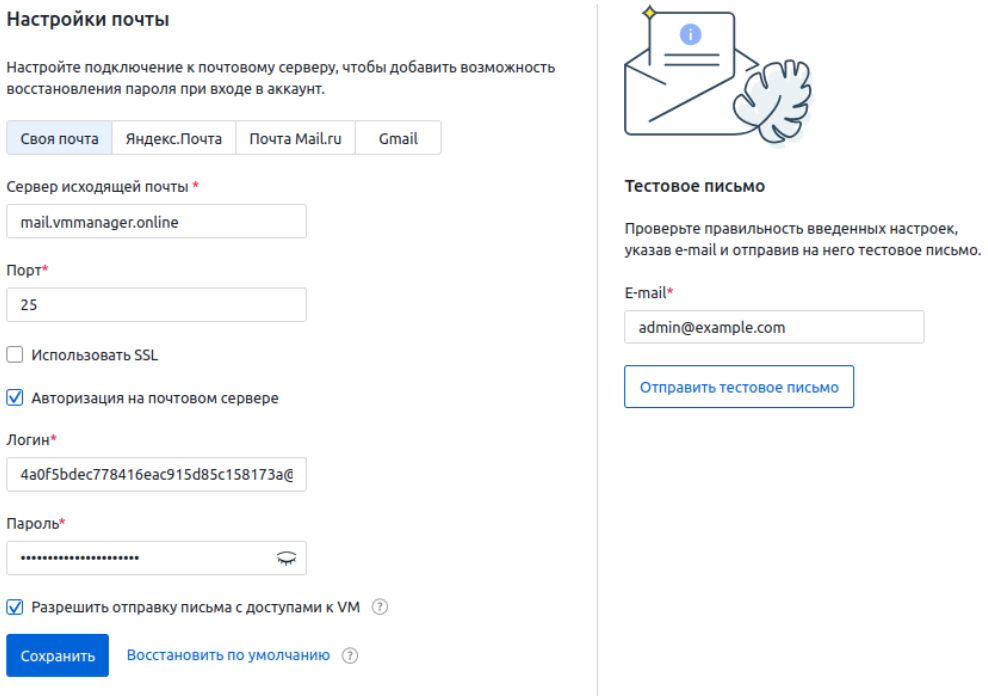

Рис. 2 — Настройка почтового сервера

2.4.3.3. Настройка клиентского сервиса

Настройка клиентского сервиса позволяет:

– указать контакты технической поддержки;

– настроить ссылки на документацию для пользователей;

– добавить ссылки на юридические документы;

– указать email для запроса на удаление персональных данных.

Порядок настройки:

1) нажать на значок «шестеренка» и перейти на вкладку «Клиентский сервис»;

2) ввести контакты техподдержки:

– email для связи с администратором;

– телефон для связи с администратором;

3) ввести URL стартовой страницы документации;

4) нажать кнопку **[Сохранить]**;

5) ввести названия документов и ссылки на них. Чтобы сделать документ обязательным для ознакомления пользователем, установить опцию «Сделать обязательным»;

6) ввести email, на который будут отправляться запросы на удаление персональных данных;

7) нажать кнопку **[Сохранить]**.

Пример настройки клиентского сервиса приведен на рис. 3.

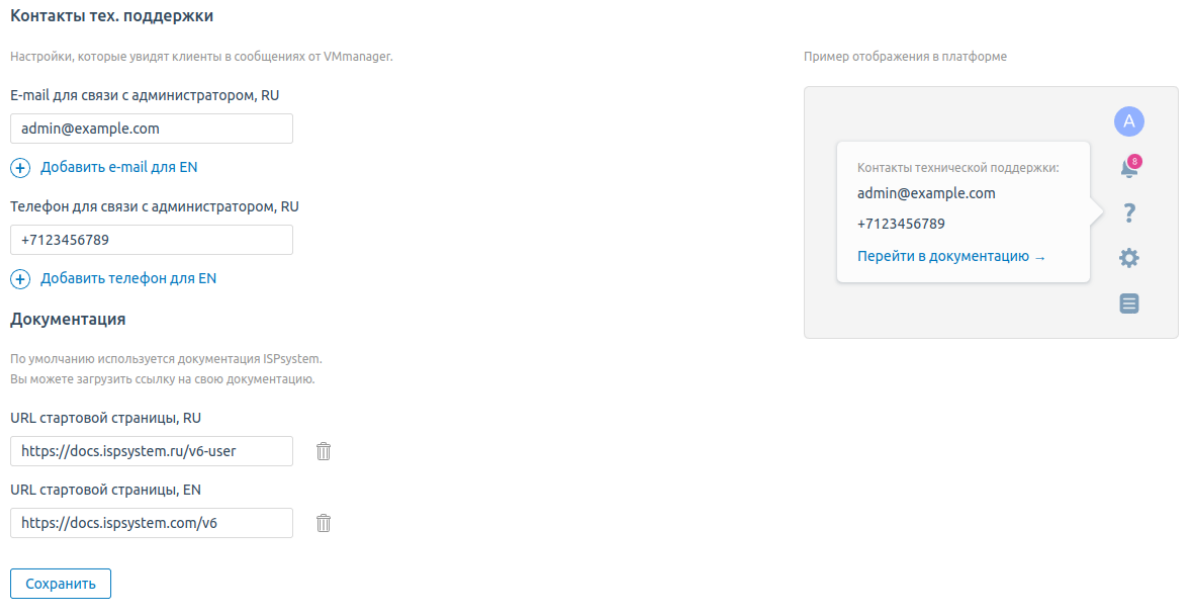

Рис. 3 — Настройка клиентского сервиса

2.4.3.4. Настройка отправки уведомлений в мессенджер «Telegram»

Платформа может использовать мессенджер «Telegram» в качестве средства оповещения пользователей о состоянии ВМ и узлов виртуализации.

Пример добавления чата приведен на рис. 4.

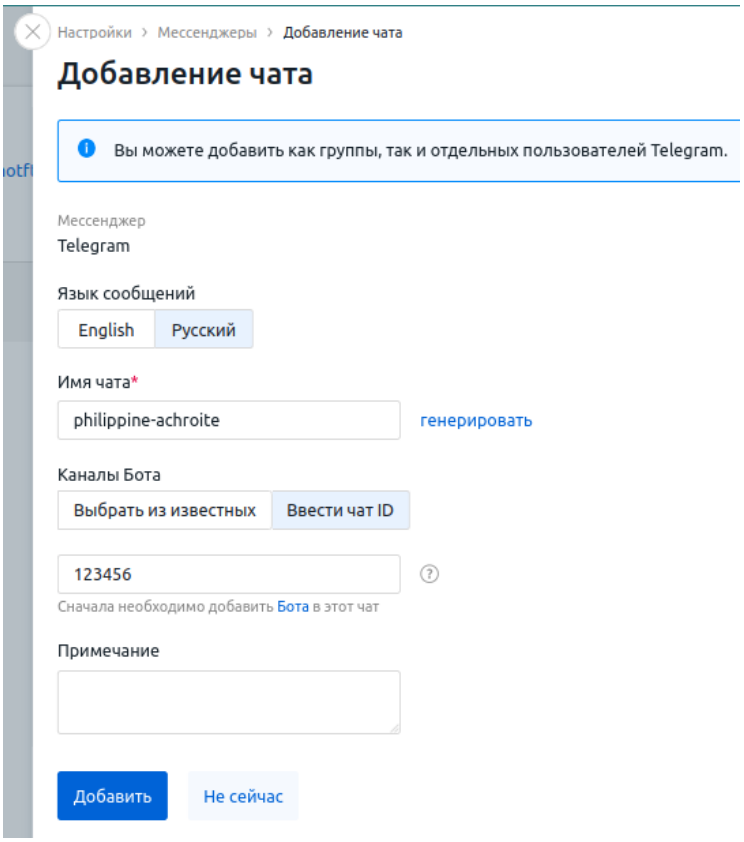

Рис. 4 — Добавление чата «Telegram»

Порядок настройки уведомлений:

1) создать бота в мессенджере «Telegram». Сохранить значение токена бота;

2) добавить созданного бота в нужные чаты «Telegram»;

3) в интерфейсе VMmanager нажать на значок «шестеренка» и перейти на вкладку «Мессенджеры»;

4) нажать кнопку **[Подключить Telegram]**;

5) ввести сохраненный токен в поле «Токен бота»;

6) нажать кнопку **[Активировать]**;

7) нажать кнопку **[Добавить чат]**;

8) выбрать язык сообщений;

9) ввести имя чата;

10) выбрать нужные чаты из списка или ввести чат ID для отправки уведомлений;

11) нажать кнопку **[Добавить]**.

2.4.3.5. Настройка резервного копирования платформы

Резервная копия программы содержит все настройки платформы и используется для восстановления работоспособности программы при сбоях. Предусмотрено создание резервных копий программы по расписанию. Порядок настройки резервного копирования:

1) нажать на значок «шестеренка» и перейти на вкладку «Резервное копирование»;

2) нажать кнопку **[Добавить расписание]**;

3) выбрать периодичность создания резервных копий:

– «Ежедневно» — требуется ввести время создания;

– «Еженедельно» — требуется ввести день недели и время создания;

– «Ежемесячно» — требуется ввести день месяца и время создания;

– «cron» — требуется ввести дату и время в формате планировщика cron;

4) ввести произвольное название расписания;

5) ввести произвольное примечание к расписанию;

6) выбрать хранилище резервных копий:

– «по SSH» — требуется ввести настройки подключения к внешнему серверу по SSH и директорию хранения;

– «по FTP» — требуется ввести настройки подключения к внешнему серверу по FTP и директорию хранения;

– «Хранить локально» — копии будут сохраняться на сервере платформы;

7) нажать кнопку **[Добавить]**.

Пример создания расписания приведен на рис. 5.

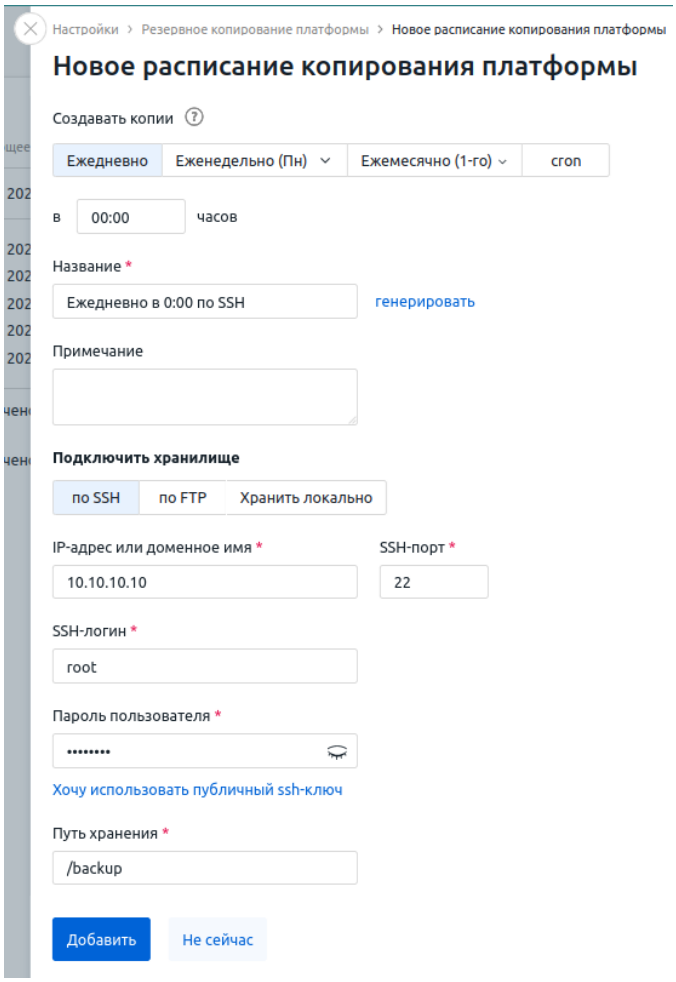

Рис. 5 — Создание расписания резервного копирования

2.4.3.6. Настройка часового пояса

По умолчанию история действий в платформе отображается по времени UTC. Поддерживается возможность включить отображение времени по локальному часовому поясу.

Порядок настройки:

1) нажать на значок «шестеренка» и перейти на вкладку «Глобальные настройки»;

2) выбрать часовой пояс. Чтобы использовать часовой пояс из настроек браузера, установить опцию «Определять на основе времени браузера».

Пример настройки часового пояса приведен на рис. 6.

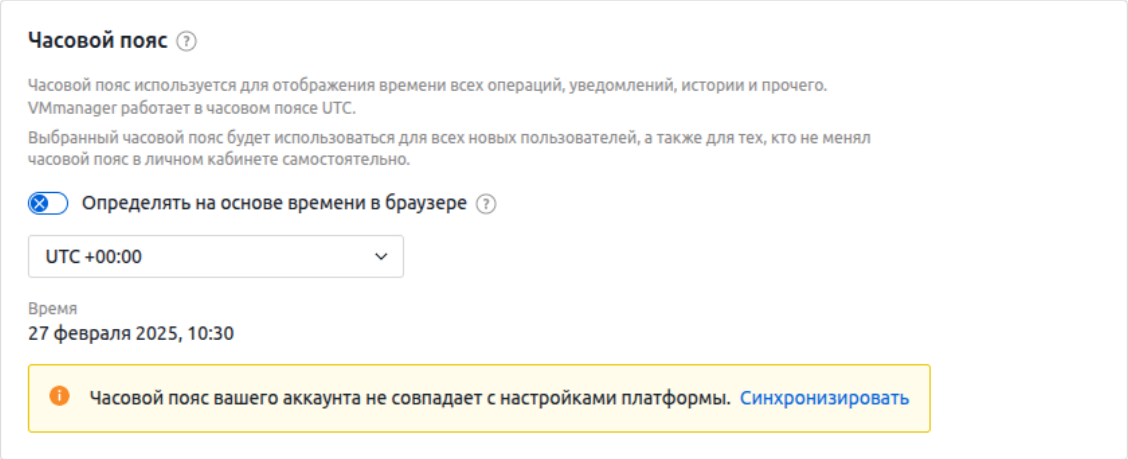

Рис. 6 — Настройка часового пояса

2.4.4. Настройка учетных записей

2.4.4.1. Создание учетных записей

Платформа позволяет создавать учетные записи следующих уровней:

– администратор — доступно управление учетными записями пользователей программы, ВМ и виртуальным оборудованием. Соответствует роли администратора средства виртуализации, определенной требованиями ФСТЭК России;

– продвинутый пользователь — доступны расширенные функции для работы с ВМ. Соответствует роли разработчика ВМ, определенной требованиями ФСТЭК России;

– пользователь — доступны базовые функции для работы с ВМ. Соответствует роли администратора ВМ, определенной требованиями ФСТЭК России.

Порядок создания учетных записей:

1) перейти в раздел «Пользователи»;
2) нажать кнопку **[Новый пользователь]**;
3) выбрать действие:
   – «Приглашение пользователей» — требуется ввести email пользователя. Письмо с приглашением будет отправлено пользователю на email. Для регистрации пользователю нужно будет перейти по ссылке из письма и самостоятельно придумать пароль;
   – «Создание пользователей» — требуется ввести пароль при создании пользователя;
4) выбрать группы для учетной записи;
5) выбрать роль пользователя в системе;

6) для приглашения пользователя ввести его email;

7) для создания пользователя ввести или сгенерировать его пароль;

8) нажать кнопку **[Пригласить]** или **[Создать]**.

Пример создания пользователя приведен на рис. 7.

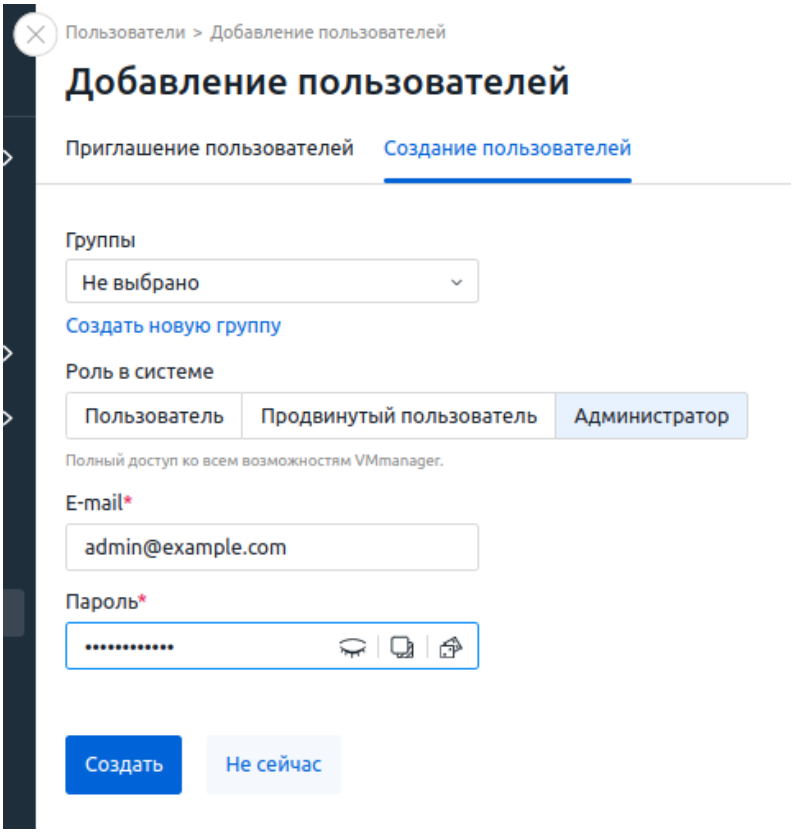

Рис. 7 — Создание пользователя

2.4.4.2. Создание групп пользователей

Пользователи платформы могут быть логически объединены в группы. Для каждой группы существует возможность указать список IP-адресов и подсетей, с которых пользователи могут быть авторизованы. Порядок создания группы пользователей:

1) перейти в раздел «Пользователи — Группы пользователей»;

2) нажать кнопку **[Создать группу]**;

3) ввести параметры группы:

   – название;

   – IP-адреса для доступа к платформе;

4) нажать кнопку **[Сохранить]**;

5) нажать кнопку **[Изменить участников группы]**;

6) выделить учетные записи, которые нужно добавить;

7) нажать кнопку **[Сохранить изменения]**.

Пример создания группы пользователей приведен на рис. 8.

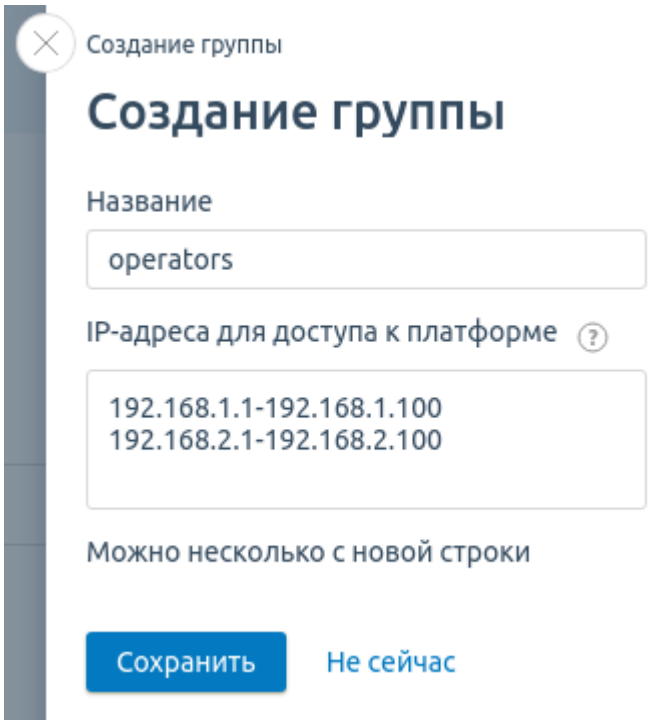

Рис. 8 — Создание группы пользователей

2.4.4.3. Синхронизация учетных записей с LDAP

Синхронизация учетных записей с LDAP позволяет автоматически добавлять в платформу учетные записи из каталогов LDAP различных реализаций. Порядок настройки синхронизации:

1) нажать на значок «шестеренка» и перейти на вкладку «Синхронизация с LDAP»;
2) выбрать реализацию каталога LDAP — «FreeIPA»;
3) ввести настройки подключения:
   а) Base DN — объект каталога, с которого начинается поиск;
   б) для подключения по SSL установить опцию «Использовать SSL для подключения»;
   в) адрес основного сервера;
   г) порт подключения;
   д) Bind DN — уникальное имя для аутентификации;
   е) пароль;
   ж) для стандартной реализации LDAP ввести:
      – Users DN — параметр для поиска и загрузки пользователей;
      – Groups DN — параметр для поиска и загрузки групп пользователей;
      – Groupname attribute — атрибут для загрузки имени группы;

– email attribute — атрибут для загрузки адреса электронной почты пользователя;

4) нажать кнопку **[Далее]**;

5) выбрать DN группы для всех ролей, используемых в платформе;

6) чтобы платформа выполняла синхронизацию по расписанию:

а) установить опцию «Синхронизировать пользователей автоматически»;

б) выбрать параметры расписания:

– «Каждый час»;

– «Ежедневно» — требуется выбрать время синхронизации;

– «Еженедельно» — требуется выбрать день недели и время синхронизации;

– «cron» — требуется ввести дату и время в формате планировщика cron;

7) нажать кнопку **[Начать синхронизацию]**.

Пример настройки подключения к LDAP приведен на рис. 9.

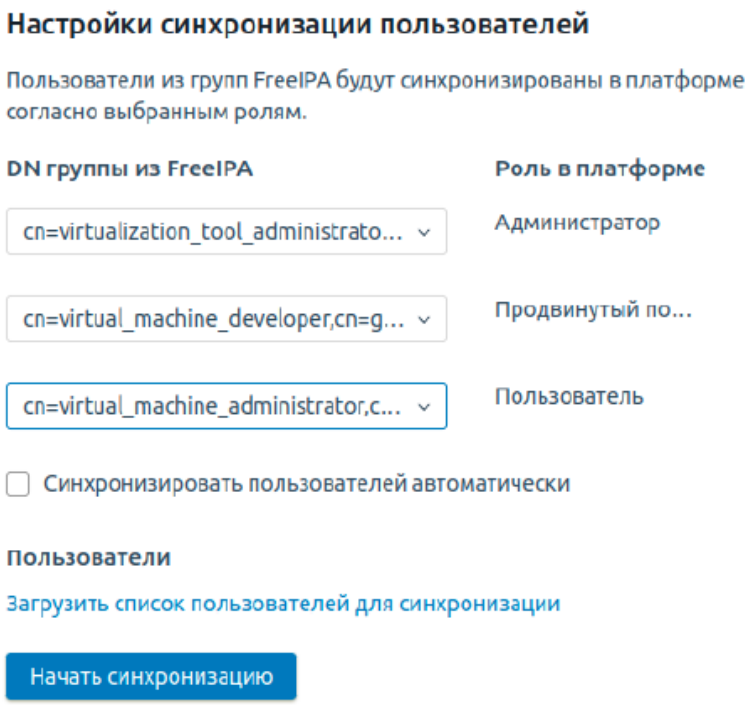

Рис. 9 — Настройка подключения к LDAP

2.4.4.4. Настройка ограничений аутентификации

Настройка ограничений аутентификации позволяет ограничить количество и периодичность неудачных попыток входа в платформу (аутентификации).

Пример настройки аутентификации приведен на рис. 10.

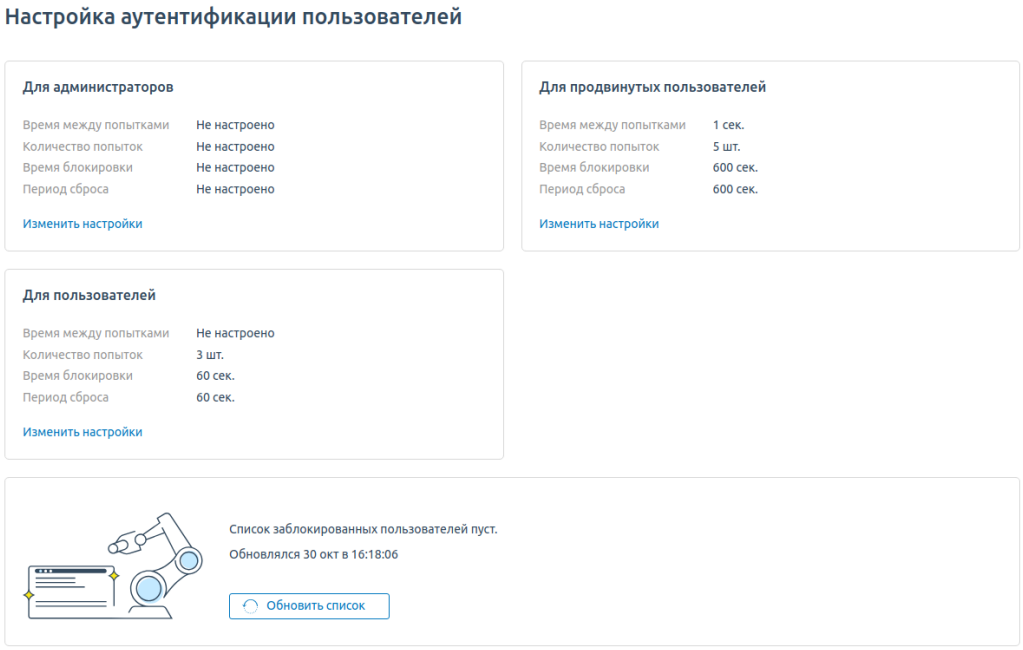

Рис. 10 — Настройка аутентификации пользователей

В настройках аутентификации могут быть заданы следующие ограничения:

– количество неудачных попыток — если пользователь сделал больше попыток ввести учетные данные, IP-адрес пользователя будет заблокирован;

– время между попытками — минимальное время после ввода неверных данных, через которое пользователь сможет повторить попытку входа.

Настройки аутентификации задаются отдельно для каждого типа учетных записей — пользователя, продвинутого пользователя и администратора.

Порядок настройки ограничений аутентификации:

1) нажать на значок «шестеренка» и перейти на вкладку «Политики безопасности»;

2) нажать кнопку **[Изменить настройки]** в нужном блоке — «Для администраторов», «Для продвинутых пользователей», «Для пользователей»;

3) ввести требуемые настройки:

– время между попытками, секунда — минимальное время после ввода неверных данных, через которое пользователь сможет повторить попытку входа;

– количество неудачных попыток, шт. — максимальное количество попыток неудачного ввода, после которого IP-адрес пользователя будет заблокирован;

– продолжительность блокировки, секунда — время, в течение которого аутентификация будет недоступна;

– период сброса, секунда — время, по истечении которого количество неудачных попыток сбросится;

4) нажать кнопку **[Сохранить]**.

2.4.4.5. Управление активными сессиями

Администратор платформы имеет возможность завершить активную сессию пользователя.

Порядок завершения сессии:

1) перейти в раздел Пользователи, открыть вкладку «Активные сессии»;
2) выбрать сессию и нажать ссылку «Завершить сессию».

Пример управления активными сессиями приведен на рис. 11.

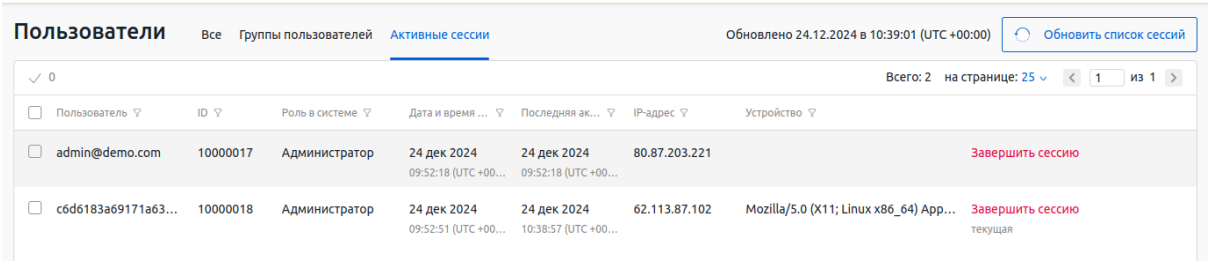

Рис. 11 — Управление активными сессиями

2.4.5. Настройка кластеров

2.4.5.1. Создание кластера

Кластер — это логическая совокупность узлов виртуализации, расположенных в одной локации.

Порядок создания кластера:

1) перейти в раздел «Кластеры»;
2) нажать кнопку **[Создать кластер]**;
3) выбрать технологию виртуализации KVM;
4) ввести или сгенерировать название кластера;
5) выбрать часовой пояс по умолчанию для узлов виртуализации и ВМ;
6) ввести DNS-серверы для ВМ;
7) ввести произвольное примечание к кластеру;
8) нажать кнопку **[Далее]**;
9) выбрать ОС, доступные для установки на ВМ;
10) чтобы к ВМ в кластере можно было подключиться по SPICE, установить опцию «Разрешить подключения по протоколу SPICE»;
11) чтобы разрешить пользователям загружать ВМ с собственных ISO-образов, установить опцию «Пользователи могут загружать свои ISO-образы»;

12) чтобы разрешить пользователям работу с виртуальными дисками, установить опцию «Пользователи могут подключать/отключать свои диски VM»;

13) выбрать шаблон доменов для ВМ;

14) чтобы разрешить владельцам ВМ изменять доменные имена, установить опцию «Пользователи могли менять доменное имя»;

15) выбрать коэффициент оверселлинга CPU;

16) выбрать коэффициент оверселлинга RAM узла;

17) ввести ограничение количества ВМ на узлах — максимальное количество ВМ, которое будет создаваться на узлах кластера;

18) выбрать тип распределения ВМ на узлах:

- равномерное — ВМ будут создаваться на самом свободном узле кластера;
- последовательное — ВМ будут создаваться на самом заполненном узле кластера;

19) нажать кнопку **[Далее]**;

20) выбрать правила настройки хранилищ на узлах кластера;

21) нажать кнопку **[Далее]**;

22) выбрать тип настройки сети;

23) нажать кнопку **[Создать]**.

Пример создания кластера приведен на рис. 12.

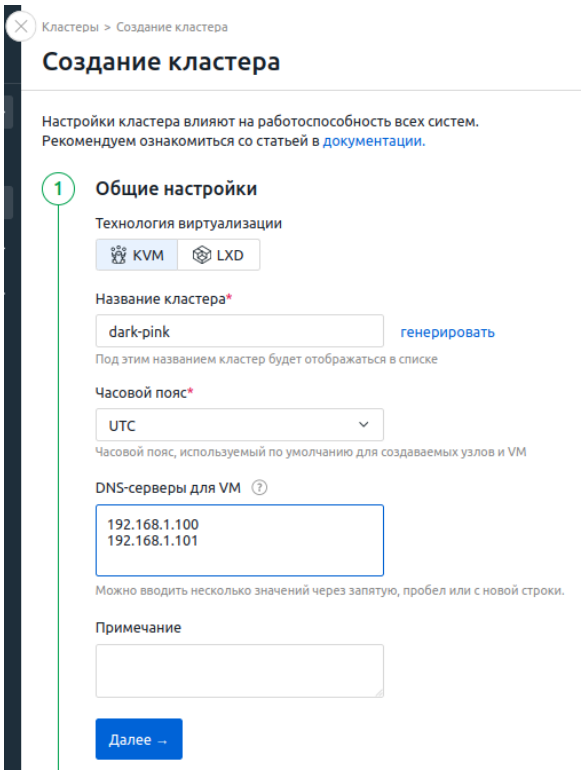

Рис. 12 — Создание кластера

2.4.5.2. Настройка и подключение узлов виртуализации

Для настройки узлов виртуализации необходимо:

1) подключиться к серверу платформы по SSH;

2) подключить ISO-образ платформы:

```
mount -o loop <path_to_iso> /mnt
```

3) запустить скрипт установки:

```
cd /mnt/vmmanager6_kvm_node && sudo sh install.sh
```

4) дождаться окончания установки. Если установка завершилась успешно, то в терминале появится сообщение вида:

```
Done. Next - add this node to VMmanager
```

Пример подключения узла виртуализации приведен на рис. 13.

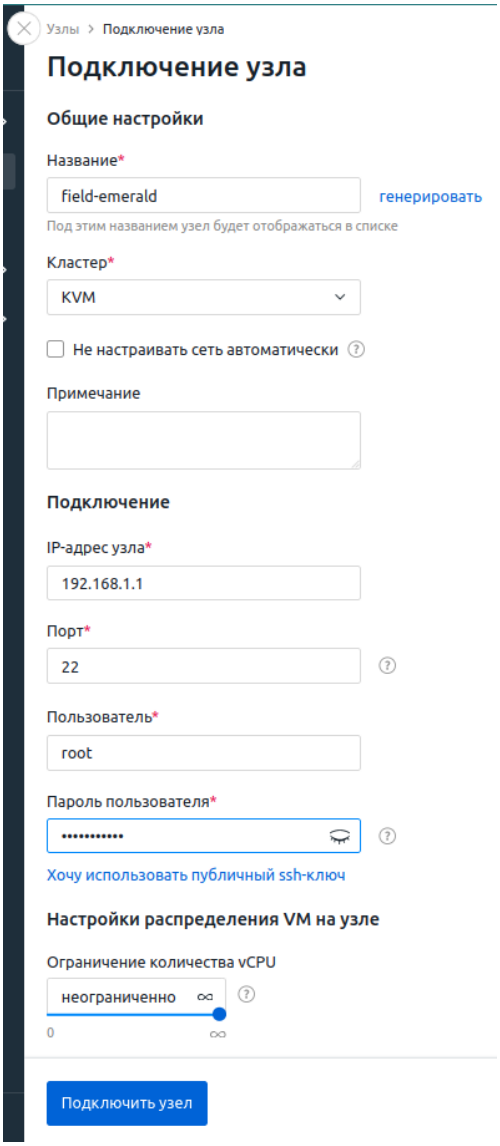

Рис. 13 — Подключение узла виртуализации

Порядок подключения узла виртуализации:

1) перейти в раздел «Узлы»;
2) нажать кнопку **[Подключить узел]**;
3) ввести название узла;
4) выбрать кластер;
5) чтобы на узле не создавался бридж по умолчанию, установить опцию «Не настраивать сеть автоматически»;
6) ввести произвольное примечание;
7) ввести IP-адрес сервера и порт для подключения по протоколу SSH;
8) ввести имя пользователя для подключения;
9) ввести пароль пользователя или добавить на сервер публичный SSH-ключ платформы;
10) ввести коэффициент оверселлинга RAM;
11) ввести ограничение количества VM**.** При достижении этого значения на узле будет запрещено создание ВМ и их миграция;
12) ввести ограничение количества vCPU — максимальное количество vCPU, которое можно выделить для ВМ на этом узле;
13) ввести параметры VM, которые будут создаваться на узле;
14) для кластеров с типом настройки сети «Маршрутизация» ввести диапазон IP-адресов для выделения ВМ;
15) выбрать скрипты, которые должны выполниться при подключении узла;
16) нажать кнопку **[Подключить узел]**;
17) для кластеров с двумя сетевыми интерфейсами:
    - выбрать интерфейс для основной сети и/или интерфейс для дополнительной сети.
    - нажать кнопку **[Продолжить]**.

2.4.5.3. Сетевые настройки узлов виртуализации

VMmanager позволяет создавать на узле виртуализации сетевые мосты (далее - бриджи) и объединять сетевые интерфейсы в бонды.

Порядок создания бриджа:

1) перейти в раздел «Узлы»;
2) выбрать узел и нажать кнопку **[Параметры]**;
3) перейти на вкладку «Настройки сети»;
4) нажать кнопку **[Добавить устройство]**;
5) выбрать тип устройства — «Бридж»;

6) ввести название бриджа;

7) ввести тег VLAN;

8) выбрать порты для объединения;

9) ввести IP-адреса и шлюзы бриджа в формате IPv4 и/или IPv6;

10) чтобы сделать бридж основным, установить опцию «Сделать бриджем по умолчанию для создания VM»;

11) нажать кнопку **[Создать];**

12) нажать кнопку **[Применить изменения];**

13) нажать кнопку **[Применить].**

Пример создания бриджа приведен на рис. 14.

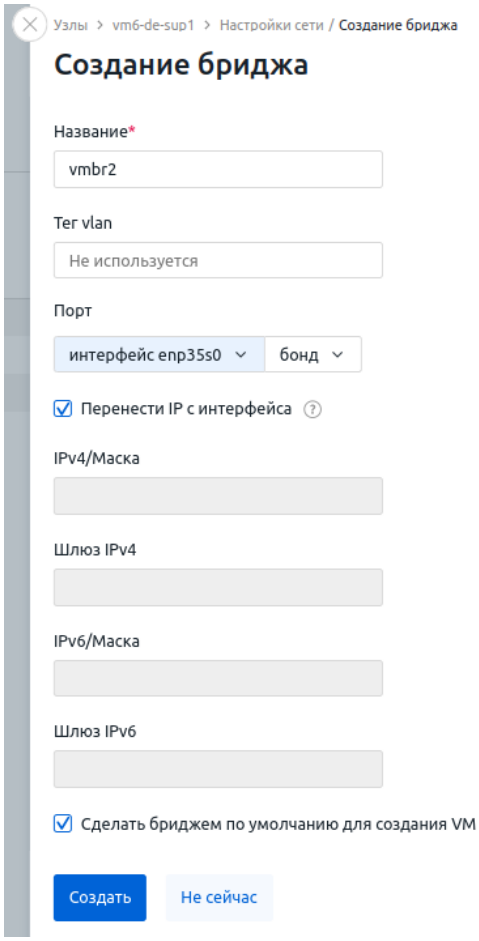

Рис. 14 — Создание бриджа

Порядок создания бонда:

1) перейти в раздел «Узлы»;

2) выбрать узел и нажать кнопку **[Параметры]**;

3) перейти на вкладку «Настройки сети»;

4) нажать кнопку **[Добавить устройство]**;

5) выбрать тип устройства — «Бонд»;

6) ввести название бонда;
7) выбрать интерфейсы для объединения;
8) ввести IP-адреса и шлюзы бонда в формате IPv4 и/или IPv6;
9) выбрать режим работы бонда;
10) нажать кнопку **[Создать];**
11) нажать кнопку **[Применить изменения];**
12) нажать кнопку **[Применить].**

Пример создания бонда приведен на рис. 15.

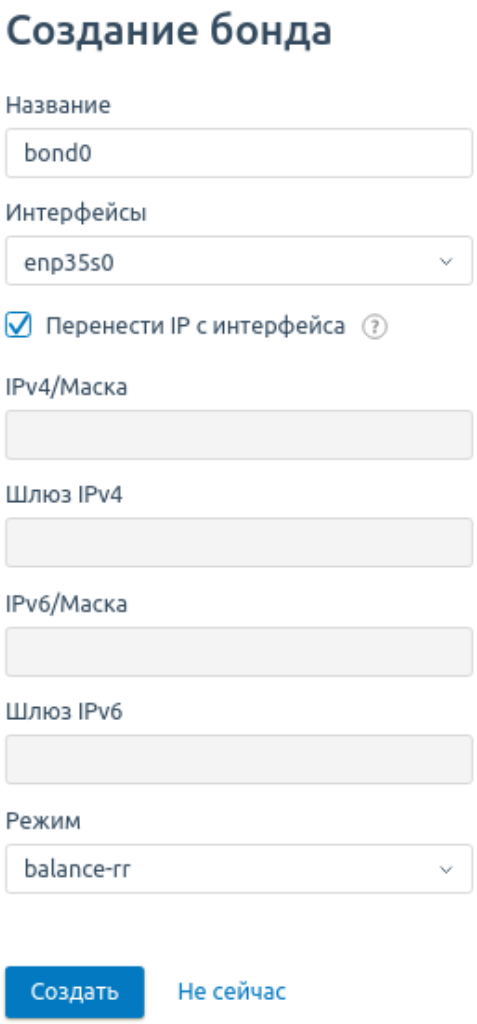

Рис. 15 — Создание бонда

2.4.5.4. Настройка распределения ВМ

При создании ВМ VMmanager выбирает узел кластера с наиболее подходящими настройками распределения.

Порядок настройки распределения:

1) перейти в раздел «Узлы»;

2) выбрать узел и нажать кнопку **[Параметры]**;

3) перейти на вкладку «Настройки распределения VM»;

4) ввести коэффициент оверселлинга RAM;

5) ввести ограничение количества VM — максимальное количество ВМ на узле;

6) ввести ограничение количества vCPU — максимальное количество vCPU, которое можно выделить для ВМ на этом узле;

7) выбрать параметры ВМ для фильтров распределения:

- теги ОС — теги шаблонов ОС;
- конфигурации — названия конфигураций;
- ресурсы RAM — объем оперативной памяти;
- ресурсы Storage — объем диска;
- ресурсы vCPU — количество виртуальных процессоров;
- сложный фильтр — условие с несколькими параметрами;

8) нажать кнопку **[Сохранить]**.

Пример настройки распределения ВМ приведен на рис. 16.

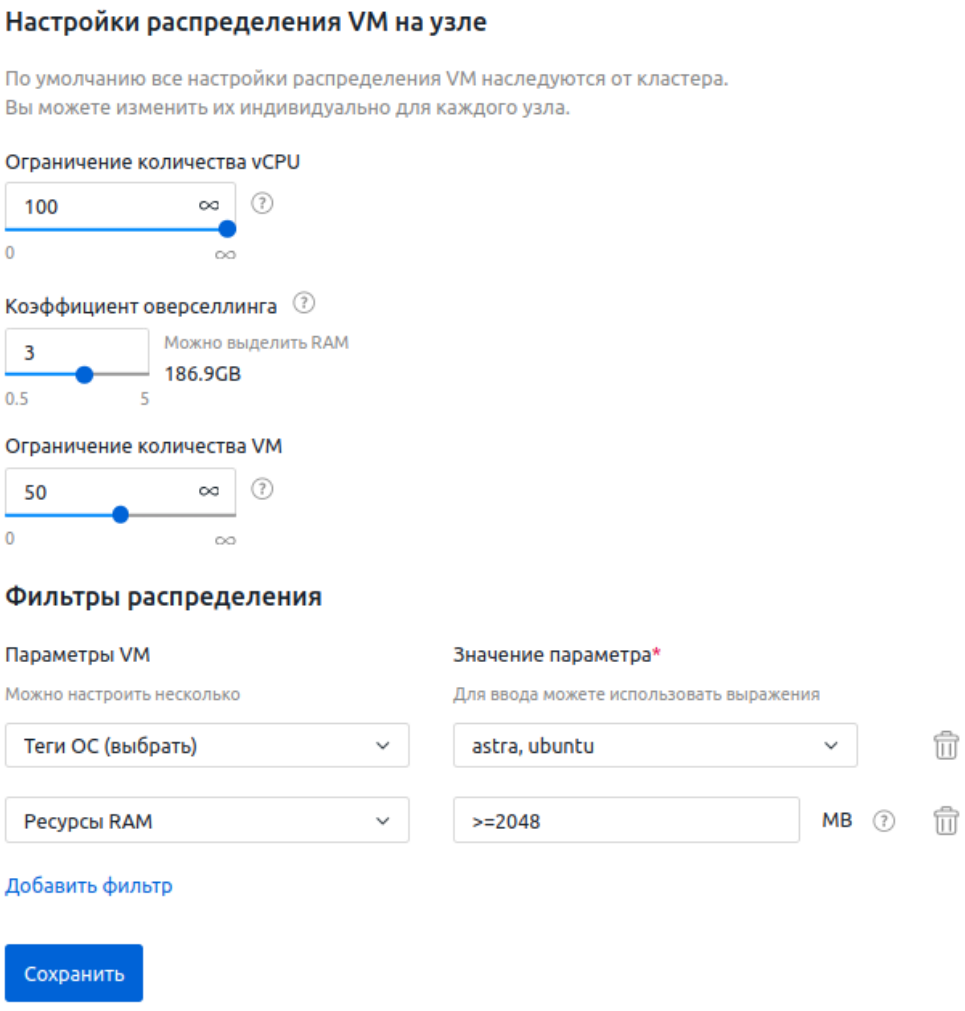

Рис. 16 — Настройки распределения ВМ

2.4.5.5. Настройка отказоустойчивости

Отказоустойчивый кластер (HA-кластер) — группа серверов, гарантирующая минимальное время простоя ВМ. В случае, если один из серверов (узлов) кластера потерял связь с другими узлами или подключенным хранилищем, VMmanager запустит процесс аварийного восстановления — релокации ВМ.

Порядок настройки отказоустойчивости:

1) перейти в раздел «Кластеры»;
2) выбрать кластер и нажать кнопку **[Параметры]**;
3) перейти на вкладку «Отказоустойчивость»;
4) нажать кнопку **[Включить отказоустойчивость]**;
5) выбрать какие ВМ должны восстанавливаться при отказе узла кластера;
6) при использовании хранилища Ceph ввести его настройки;
7) ввести IP-адрес шлюза, связь с которым будет проверяться узлом при потере связи с кластером;
8) нажать кнопку **[Сохранить]**.

2.4.5.6. Настройка хранилищ кластера

Хранилища используются для хранения дисков и образов ВМ, шаблонов ОС. VMmanager поддерживает следующие типы хранилищ:

- файловое хранилище — файловая система узла виртуализации;
- LVM — менеджер логических томов;
- Ceph — программно-определяемое отказоустойчивое распределенное сетевое хранилище;
- сетевое LVM — LVM в сети хранения данных SAN. Узлы кластера работают с хранилищем как с блочным устройством по протоколу iSCSI;
- NAS — сетевое хранилище, обеспечивающее доступ к данным на уровне файлов.

Пример добавления сетевого хранилища приведен на рис. 17.

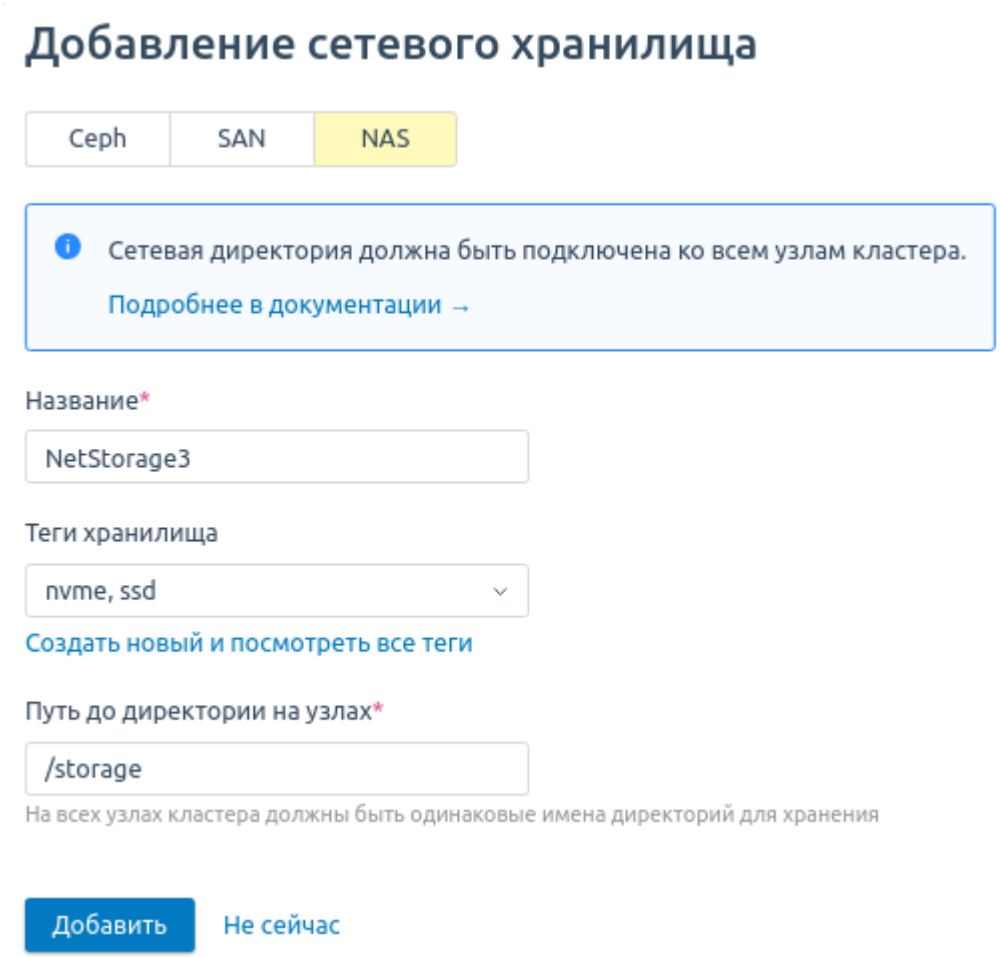

Рис. 17 — Добавление сетевого хранилища

Порядок подключения хранилища:

1) перейти в раздел «Кластеры»;
2) выбрать кластер и нажать кнопку **[Параметры]**;
3) перейти на вкладку «Локальные хранилища» или «Сетевые хранилища»;
4) нажать кнопку **[Добавить хранилище]**;
5) ввести параметры хранилища;
6) нажать кнопку **[Добавить]**.

2.4.5.7. Балансировщик

Балансировщик — это сервис, позволяющий автоматически выравнивать загрузку узлов виртуализации за счет перераспределения ВМ между узлами. Процедура распределения ВМ выполняется автоматически с периодичностью, заданной в настройках балансировщика.

Порядок включения балансировщика:

1) перейти в раздел «Кластеры»;
2) выбрать кластер и нажать кнопку **[Параметры]**;
3) перейти на вкладку «Балансировщик»;

4) нажать кнопку **[Включить балансировщик]**;

5) ввести периодичность проверки баланса в минутах.

Пример настройки балансировщика приведен на рис. 18.

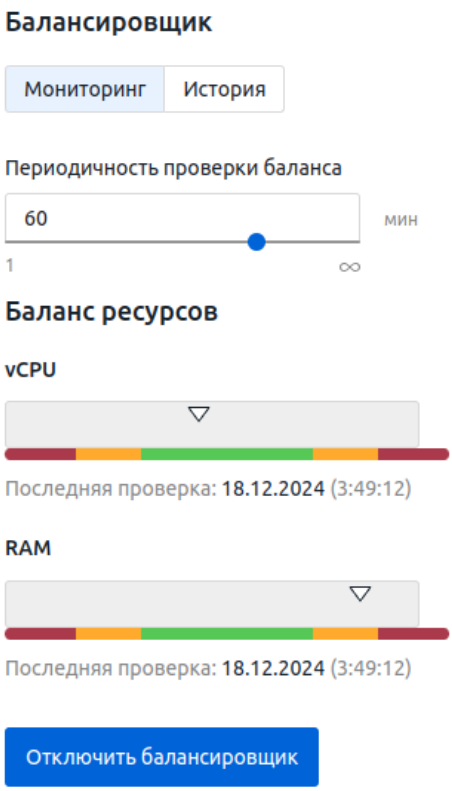

Рис. 18 — Настройка балансировщика

2.4.5.8. Режим распределенного коммутатора

Распределенный коммутатор позволяет унифицировать настройки сети на узлах кластера независимо от настроек интерфейсов на узлах и централизованно управлять ими. VMmanager позволяет создать шаблоны сетевых настроек с помощью порт-групп в распределенном коммутаторе.

Порядок включения режима:

1) перейти в раздел «Кластеры»;

2) выбрать кластер, нажать кнопку **[Параметры]** и перейти на вкладку «Настройки сети»;

3) перейти на вкладку «Распределенный коммутатор (DS)» и нажать кнопку **[Включить режим DS]**;

4) нажать кнопку **[Добавить порт-группу]**;

5) ввести настройки порт-группы:

- название;
- тег «vlan»;

– Uplink-интерфейс — интерфейс, через который на узле создаются соответствующие vlan- и бридж-интерфейсы;

– чтобы порт-группа использовалась по умолчанию для новых ВМ, установить опцию «Использовать по умолчанию для новых VM»;

– чтобы снять с интерфейса узла адреса IPv4 и IPv6 и назначить на бридж, который связан с порт-группой, установить опцию «Автоматически переносить IP с интерфейса»;

6) нажать кнопку **[Добавить]**.

Пример добавления порт-группы приведен на рис. 19.

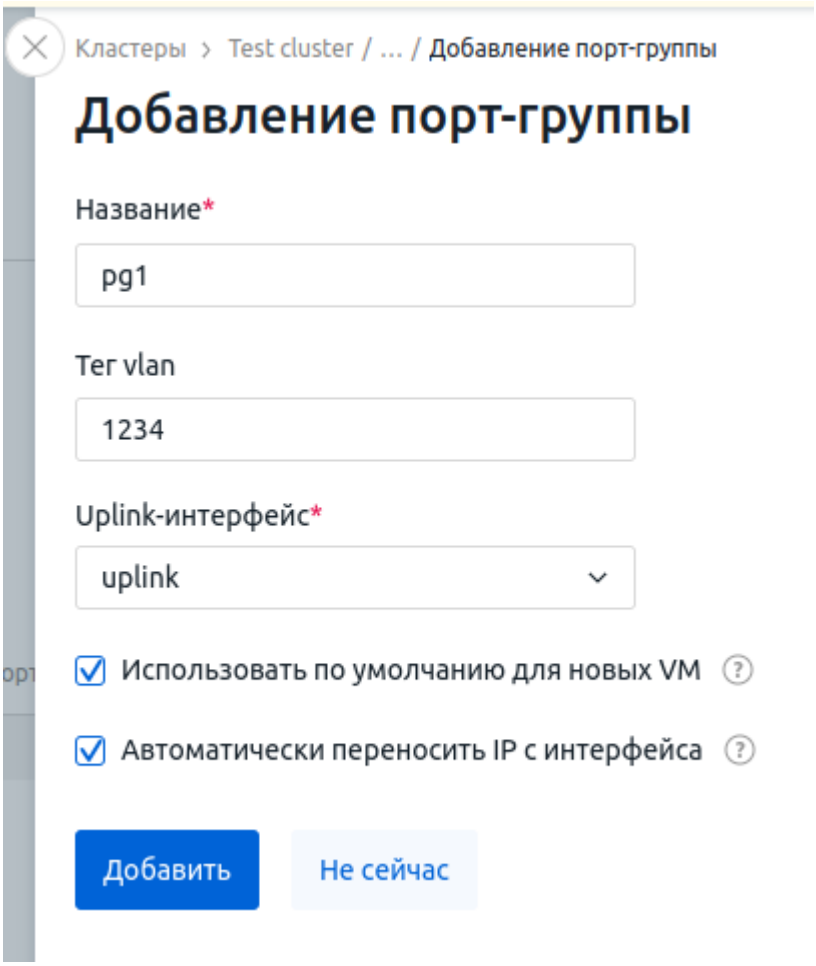

Рис. 19 — Добавление порт-группы

2.4.5.9. Режим обслуживания

Режим обслуживания используется, если на узле кластера нужно провести технические работы. На узле, находящемся в режиме обслуживания, не поддерживается:

– создание новых ВМ;

– перенос ВМ с других узлов.

При переводе узла в режим обслуживания возможно проведение эвакуации объектов — автоматической миграции ВМ, дисков, образов и резервных копий на другой

узел. После завершения обслуживания эвакуированные объекты будут возвращены на исходный узел. Если эвакуация объектов не выполняется, то при включении режима обслуживания все ВМ на этом узле будут остановлены.

Порядок включения режима обслуживания:

1) если объекты узла требуется эвакуировать, удалить снимки ВМ перед включением режима;

2) перейти в раздел «Узлы»;

3) выбрать узел, открыть меню «троеточие» и выбрать пункт «Режим обслуживания»;

4) чтобы узел перешел в режим обслуживания только после завершения всех задач на узле, снять опцию «Принудительно отменить все задачи на узле»;

5) чтобы провести эвакуацию объектов, активировать переключатель «Инициировать эвакуацию объектов с этого узла»;

6) нажать кнопку **[Включить]**. Когда узел будет готов к проведению обслуживания, его статус изменится на «В режиме обслуживания»;

7) если эвакуация каких-либо объектов завершилась с ошибкой, выполнить их миграцию вручную.

Порядок отключения режима обслуживания:

1) перейти в раздел «Узлы»;

2) выбрать узел, открыть меню «троеточие» и выбрать пункт «Режим обслуживания»;

3) если перенесенные объекты не нужно возвращать на узел, снять опцию «Вернуть эвакуированные объекты»;

4) нажать кнопку **[Отключить]**.

Пример окна настройки режима обслуживания приведен на рис. 20.

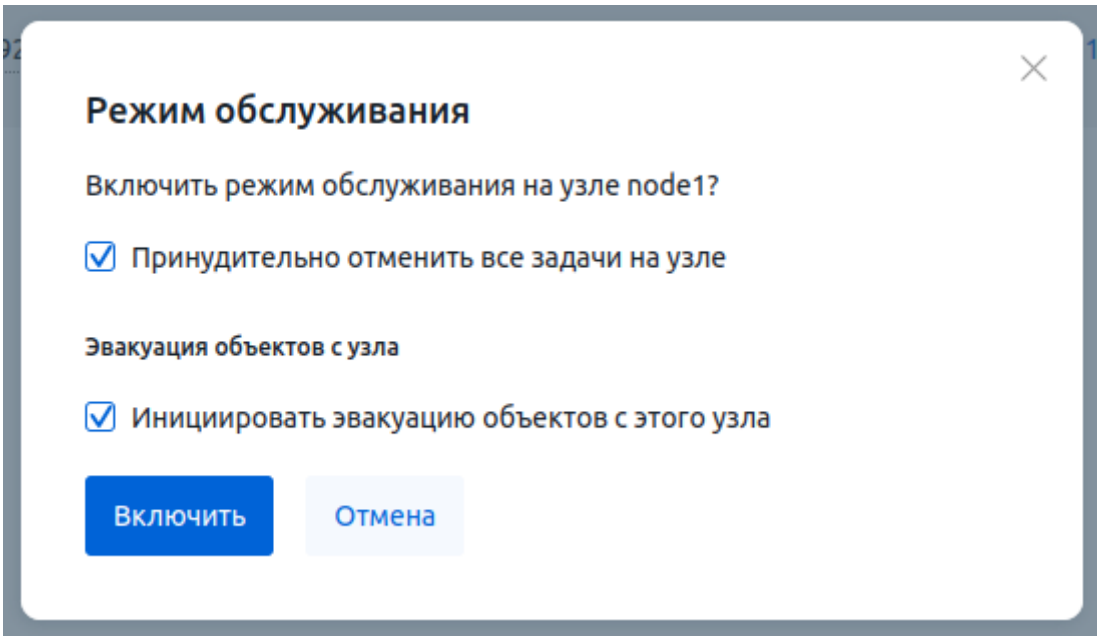

Рис. 20 — Режим обслуживания

2.4.6. Настройка адресного пространства

2.4.6.1. Создание физических сетей

Физические сети используются для учета адресного пространства, выделяемого ВМ.

Порядок создания физических сетей:

1) перейти в раздел «Сети — Физические сети»;
2) нажать кнопку **[Добавить физическую сеть]**;
3) чтобы использовать все IP-адреса сети для выдачи ВМ, включая служебные, установить опцию «Не занимать служебные IP-адреса»;
4) ввести сеть в формате IPv4 или IPv6;
5) ввести IP-адрес шлюза;
6) ввести произвольное примечание к сети;
7) нажать кнопку **[Добавить]**.

Пример добавления физической сети приведен на рис. 21.

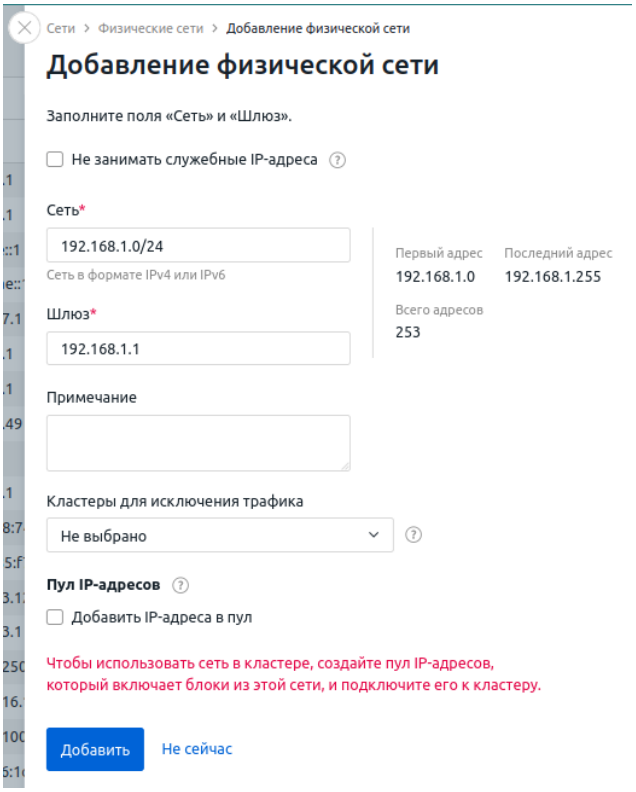

Рис. 21 — Добавление физической сети

2.4.6.2. Создание пулов IP-адресов

Пулы логически объединяют блоки IP-адресов. Это позволяет разделить блоки адресов на публичные и приватные, разрешить использовать на определенных кластерах только необходимые блоки.

Порядок создания пулов IP-адресов:

1) перейти в раздел «Сети — Пулы IP-адресов»;
2) нажать кнопку **[Создать пул IP-адресов]**;
3) ввести или сгенерировать название пула;
4) ввести IP-адреса для создания ВМ;
5) выбрать в каких кластерах пул будет доступен;
6) ввести произвольное примечание к пулу;
7) нажать кнопку **[Создать пул]**.

Пример создания пула приведен на рис. 22.

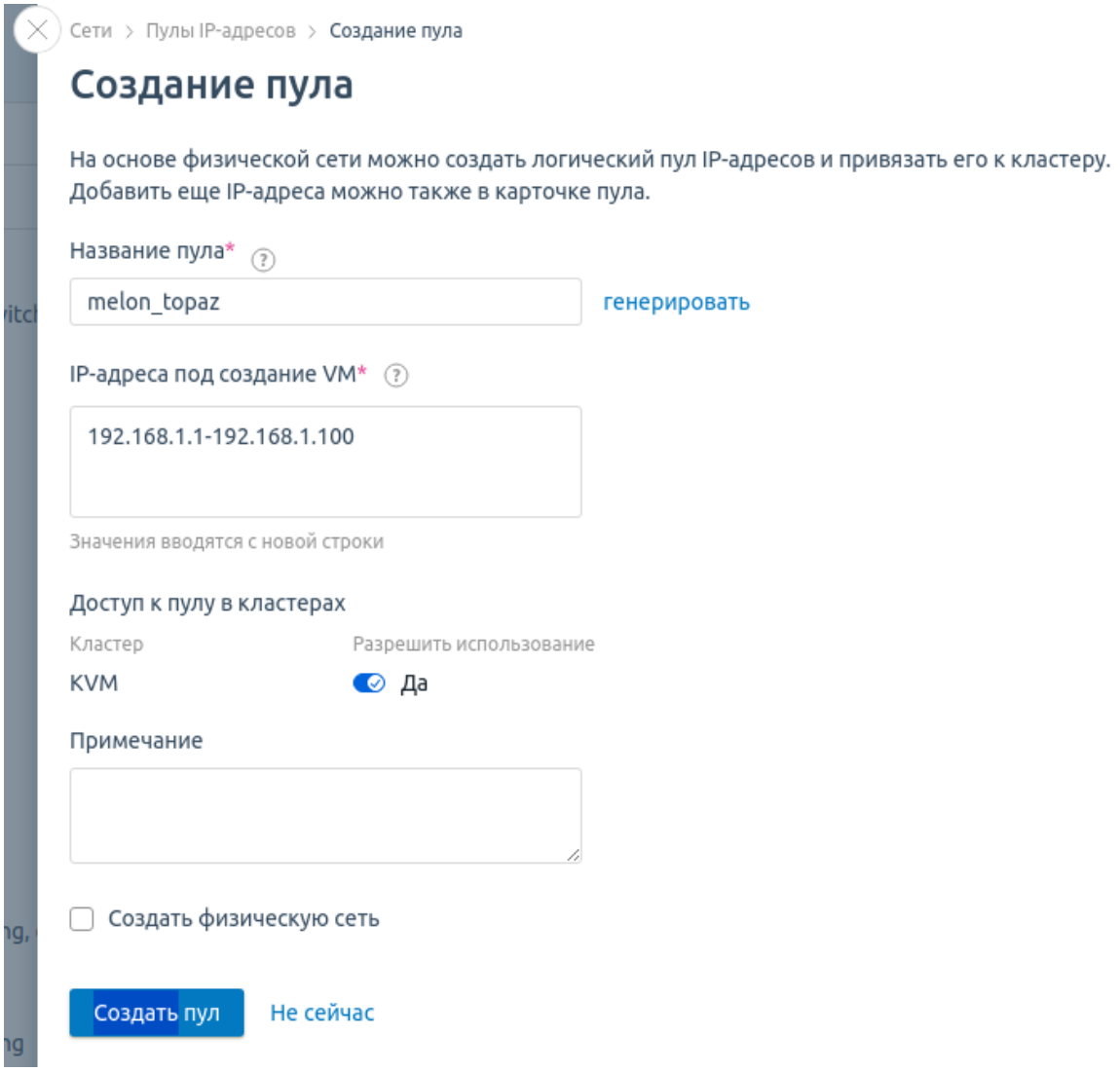

Рис. 22 — Создание пула

2.4.6.3. Настройка DNSBL

VMmanager позволяет выполнять проверку IP-адресов на их наличие в DNSBL. IP-адрес получает статус «Заблокирован DNSBL», если присутствует хотя бы в одном списке. Заблокированный IP-адрес не может быть назначен ВМ.

Порядок добавления DNSBL:

1) перейти в раздел «Сети — DNSBL»;
2) нажать кнопку **[Добавить DNSBL]**;
3) ввести доменное имя DNSBL;
4) нажать кнопку **[Добавить]**.

Пример добавления DNSBL приведен на рис. 23.

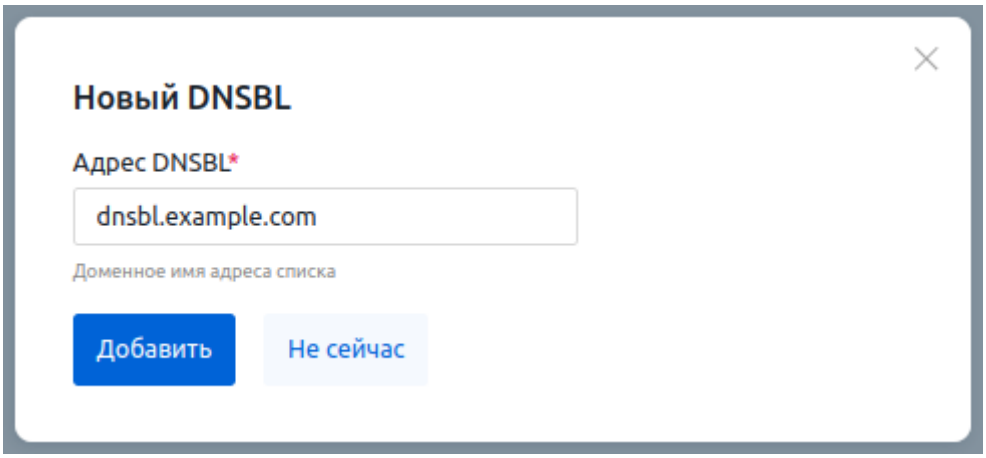

Рис. 23 — Добавление DNSBL

2.4.7. Настройка шаблонов

2.4.7.1. Настройка репозиториев ОС

Репозиторий ОС – это централизованное цифровое хранилище для шаблонов ОС и ISO-образов. По умолчанию в программе доступен локальный репозиторий, в котором находится шаблон NoOS, который используется для создания ВМ без ОС.

В директории репозитория должны находиться:

– файл `metadata.json` — файл описания репозитория;

– архив шаблонов ОС с расширением .xz.

Порядок подготовки шаблона:

1) создать ВМ с нужной версией ОС;

2) настроить ОС и установить необходимые пакеты ПО;

3) остановить ВМ;

4) определить, в каком формате сохранен диск ВМ:

```
qemu-img info <disk_path> | grep "file format"
```

5) скопировать файл диска ВМ в отдельную директорию. Если диск сохранен не в формате RAW, конвертировать его в формат RAW:

```
qemu-img convert -f <disk_format> -O raw <disk_path> <image_path>
```

6) оптимизировать файл образа с помощью утилиты virt-sparsify:

```
LIBGUESTFS_BACKEND=direct virt-sparsify --in-place <image_path>
```

7) очистить образ от персональной информации с помощью утилиты virt-sysprep:

```
LIBGUESTFS_BACKEND=direct virt-sysprep --format=raw --operations <sysprep_ops> --add <image_path> --root-password random
```

8) чтобы у ВМ, создаваемых из шаблона, был уникальный параметр machine-id, выполнить команду:

```
LIBGUESTFS_BACKEND=direct virt-sysprep --format=raw --operations machine-id --add <image_path> --root-password random
```

9) создать архив с образом с расширением .xz:

```
xz <image_path>
```

10) скопировать архив в директорию репозитория;

11) добаваить информацию о шаблоне в файл описания репозитория `metadata.json`.

Порядок добавления репозитория:

1) перейти в раздел «Шаблоны — Репозитории»;
2) нажать кнопку **[Добавить репозиторий]**;
3) ввести или сгенерировать название репозитория;
4) ввести URL репозитория;
5) нажать кнопку **[Добавить]**.

2.4.7.2. Шаблоны ОС

Для установки ОС на ВМ VMmanager использует шаблоны ОС. Шаблоны ОС в VMmanager — образы дисков ВМ с установленной ОС без дополнительного ПО и специальных настроек («чистая» ОС).

Образы хранятся в архивах с расширением .xz с максимальным сжатием и загружаются на узел кластера при первой установке ОС на ВМ.

Порядок управления шаблонами ОС:

1) перейти в раздел «Шаблоны — Операционные системы»;
2) нажать на название ОС;
3) выбрать кластеры, в которых должен быть доступен шаблон;
4) чтобы шаблон был доступен только для администратора платформы, установить опцию «Только администратор может устанавливать VM из ОС»;
5) нажать кнопку **[Сохранить]**.

Пример настройки шаблона ОС приведен на рис. 24.

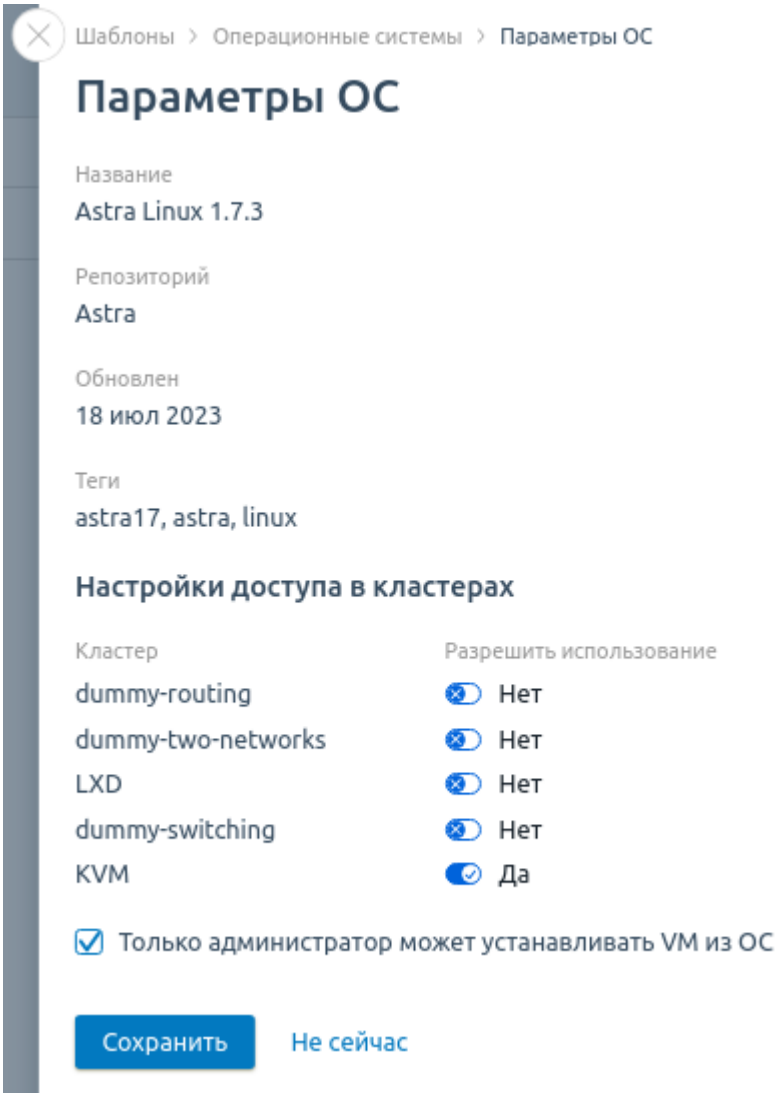

Рис. 24 — Настройка шаблона ОС

2.4.7.3. Пользовательские образы ВМ

Пользовательский образ — образ диска ВМ, который используется для создания новых ВМ.

Порядок управления образами:

1) перейти в раздел «Шаблоны — Образы VM». В данном разделе находятся образы виртуальных машин, созданные пользователями;
2) нажать на название образа;
3) ввести название образа;
4) выбрать владельца образа;
5) выбрать кому разрешен доступ к образу;
6) ввести произвольное примечание;
7) нажать кнопку **[Сохранить]**.

Пример редактирования образа ВМ приведен на рис. 25.

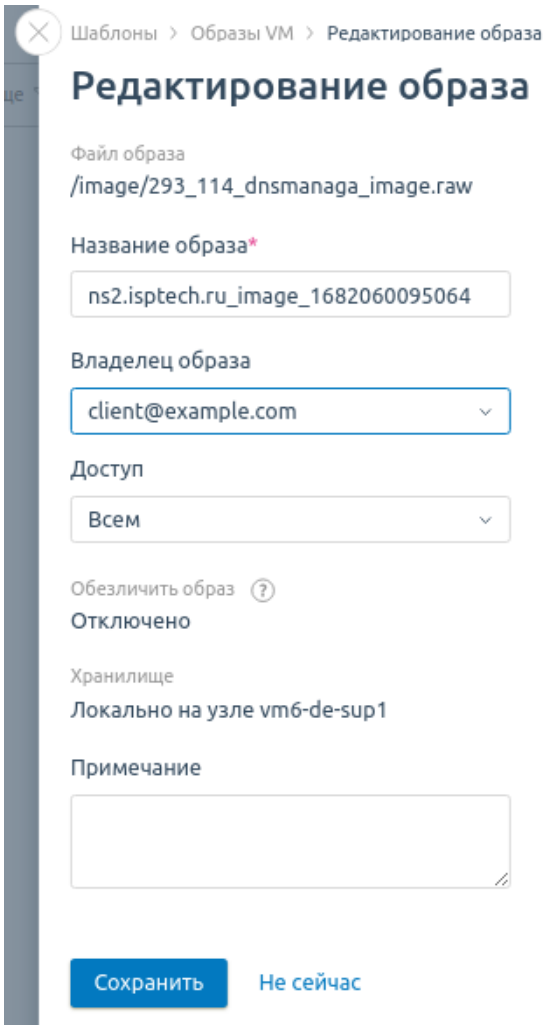

Рис. 25 — Редактирование образа ВМ

2.4.7.4. Конфигурации ВМ

Конфигурации ВМ — наборы ресурсов, которые используются для создания ВМ.

Порядок создания конфигурации:

1) перейти в раздел «Шаблоны — Конфигурации VM»;
2) нажать кнопку **[Добавить конфигурацию]**;
3) ввести название конфигурации;
4) выбрать параметры конфигурации;
5) нажать кнопку **[Добавить]**.

Пример создания конфигурации ВМ приведен на рис. 26.

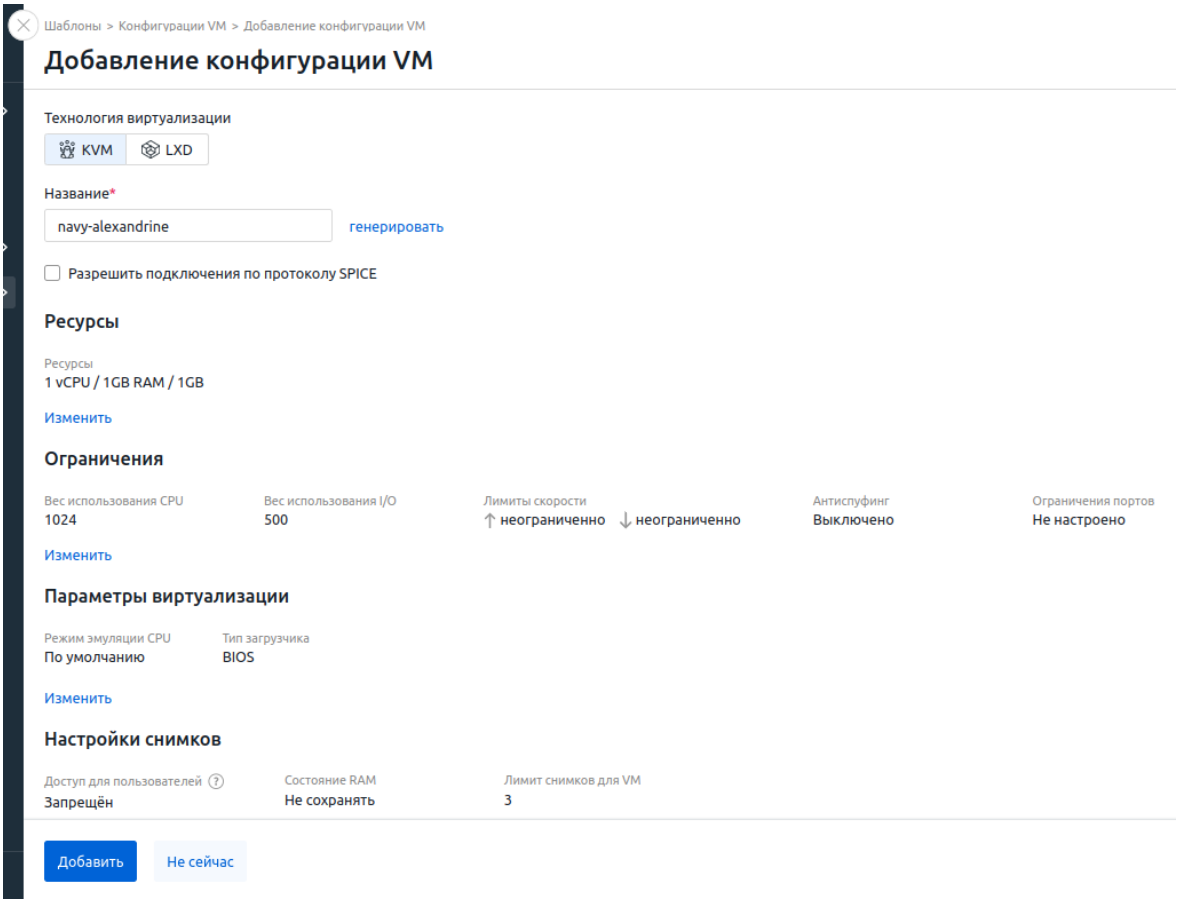

Рис. 26 — Создание конфигурации ВМ

2.4.8. Настройка ВМ

2.4.8.1. Настройка сети на ВМ

При создании ВМ VMmanager выделяет ей IP-адрес из заданного пула. Существует возможность назначить дополнительные IP-адреса для ВМ и выбрать модель добавления IP-адресов.

Пример настройки сети на ВМ приведен на рис. 27.

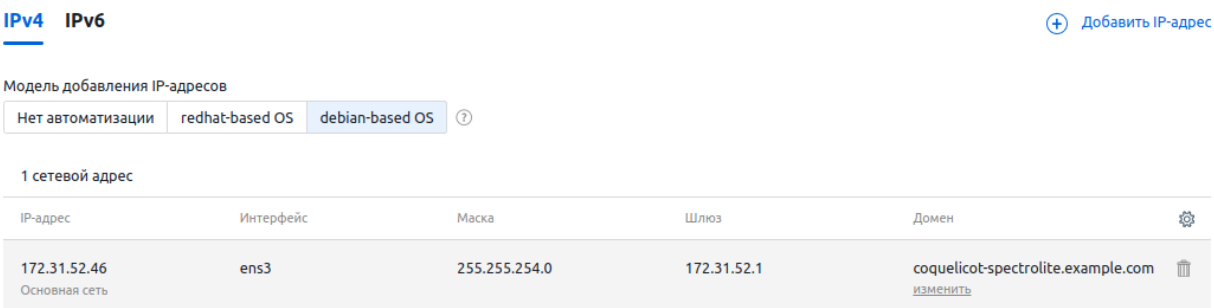

Рис. 27 — Настройка сети на ВМ

Порядок настройки IP-адресов:

1) перейти в раздел «Виртуальные машины»;
2) выбрать ВМ и нажать кнопку **[Параметры]**;

3) перейти на вкладку «**IP-адреса»;**

4) выбрать модель добавления IP-адресов:

- «debian-based» — для ОС на основе Debian;
- «freebsd-based» — для ОС на основе FreeBSD;
- «redhat-based» — для ОС на основе RHEL;
- «Windows» — для ОС семейства Windows;
- «Нет автоматизации» — для ОС, загруженных из ISO-образов и ОС семейства Windows;

5) для добавления IPv4-адреса:

- перейти на вкладку «IPv4»;
- нажать кнопку **[Добавить IP-адрес]**;
- выбрать пул, из которого будет выделены IP-адреса, или выбрать пункт «Назначить IP», чтобы ввести конкретный адрес;
- выбрать нужное количество адресов IPv4;
- нажать кнопку **[Добавить];**

6) для добавления IPv6-адреса:

- перейти на вкладку «IPv6»;
- нажать кнопку **[Включить IPv6]**;
- выбрать пул IPv6-адресов, из которого будет выделены IP-адреса;
- выбрать префикс выделяемой подсети от «/32» до «/125»;
- нажать кнопку **[Включить IPv6]**.

2.4.8.2. Управление дисками ВМ

VMmanager позволяет подключить к ВМ дополнительные виртуальные диски с контроллером:

- VirtIO — для подключения требуется установка драйвера в ОС;
- SCSI — поддерживается всеми современными ОС. К одной ВМ можно подключить не более 14 дисков этого типа;
- IDE — поддерживается всеми ОС. К одной ВМ можно подключить не более трех дисков этого типа.

Порядок добавления дисков:

1) перейти в раздел «Виртуальные машины — Диски VM»;
2) нажать кнопку **[Создать виртуальный диск]**;
3) ввести параметры диска:
   а) название диска;
   б) размер в гигабайтах;

в) раздел для увеличения при изменении параметра Storage;

4) для создания диска:

а) без подключения к ВМ:

- нажать кнопку **[Без подключения]**;
- выбрать владельца диска;
- выбрать хранилище;
- выбрать узел кластера;
- нажать кнопку **[Создать без подключения]**;

б) с подключением к ВМ:

- нажать кнопку **[Выбрать VM];**
- выбрать ВМ для подключения диска;
- если требуется, установить опцию «Сделать основным»;
- выбрать тип подключения;
- определить приоритет загрузки дисков;
- выбрать хранилище;
- нажать кнопку **[Подключить диск]**. Если подключение требует перезагрузки ВМ, кнопка будет называться **[Перезапустить VM и подключить диск]**;

5) чтобы ВМ могла работать с диском, создать на диске загрузочную запись и разделы средствами ОС.

Пример создания виртуального диска приведен на рис. 28.

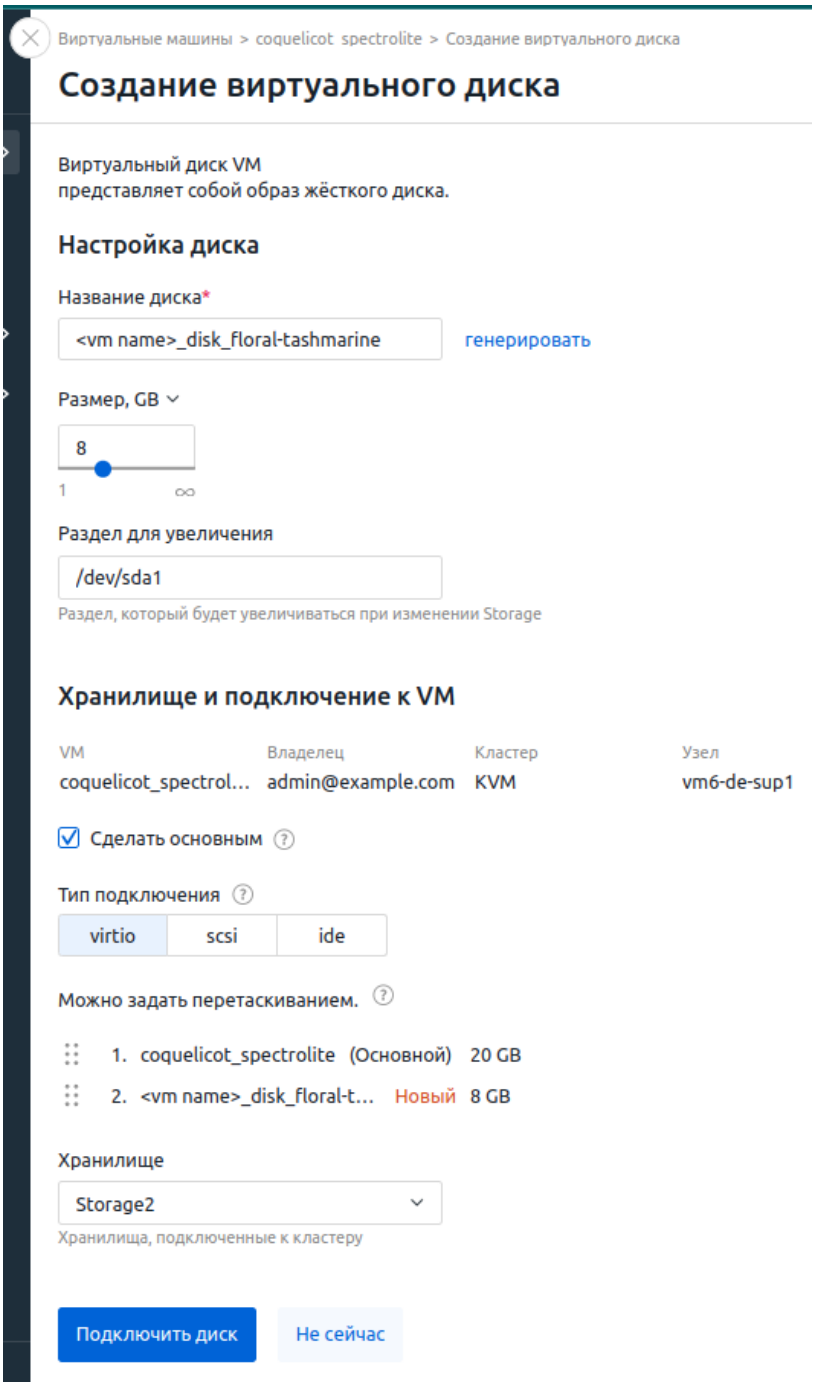

Рис. 28 — Создание виртуального диска

2.4.8.3. Запуск скриптов на ВМ

Скрипты позволяют автоматически настраивать ВМ: устанавливать ПО, изменять конфигурационные файлы и т.д.

Возможен запуск предустановленных скриптов или создание собственных. Для запуска на ОС семейства Linux скрипт должен быть написан на языке bash, на ОС Windows — на языке Powershell.

Порядок создания скриптов:

1) перейти в раздел «Скрипты»;

2) нажать кнопку **[Создать скрипт]**;

3) ввести название скрипта;

4) выбрать владельца скрипта;

5) выбрать, кому разрешен доступ к образу;

6) чтобы только владелец скрипта и администраторы платформы могли просматривать код скрипта и создавать его копии, установить опцию «Скрывать содержимое скрипта»;

7) ввести краткое описание скрипта для отображения в списке скриптов;

8) выбрать фильтры для выполнения скрипта. Скрипт доступен для запуска на ВМ при совпадении условий всех фильтров. Фильтр «Теги ОС» является обязательным, остальные — опциональными;

9) если требуется, добавить параметры скрипта;

10) выбрать тип скрипта:

- «Shell» — для ОС семейства Linux;
- «Powershell» — для ОС Windows;

11) ввести тело скрипта в окне редактора;

12) чтобы после выполнения скрипта на почту пользователю было отправлено письмо, нажать кнопку **[Добавить]** в разделе «Уведомление на email» и указать параметры письма;

13) нажать кнопку **[Создать]**.

Пример создания скрипта приведен на рис. 29.

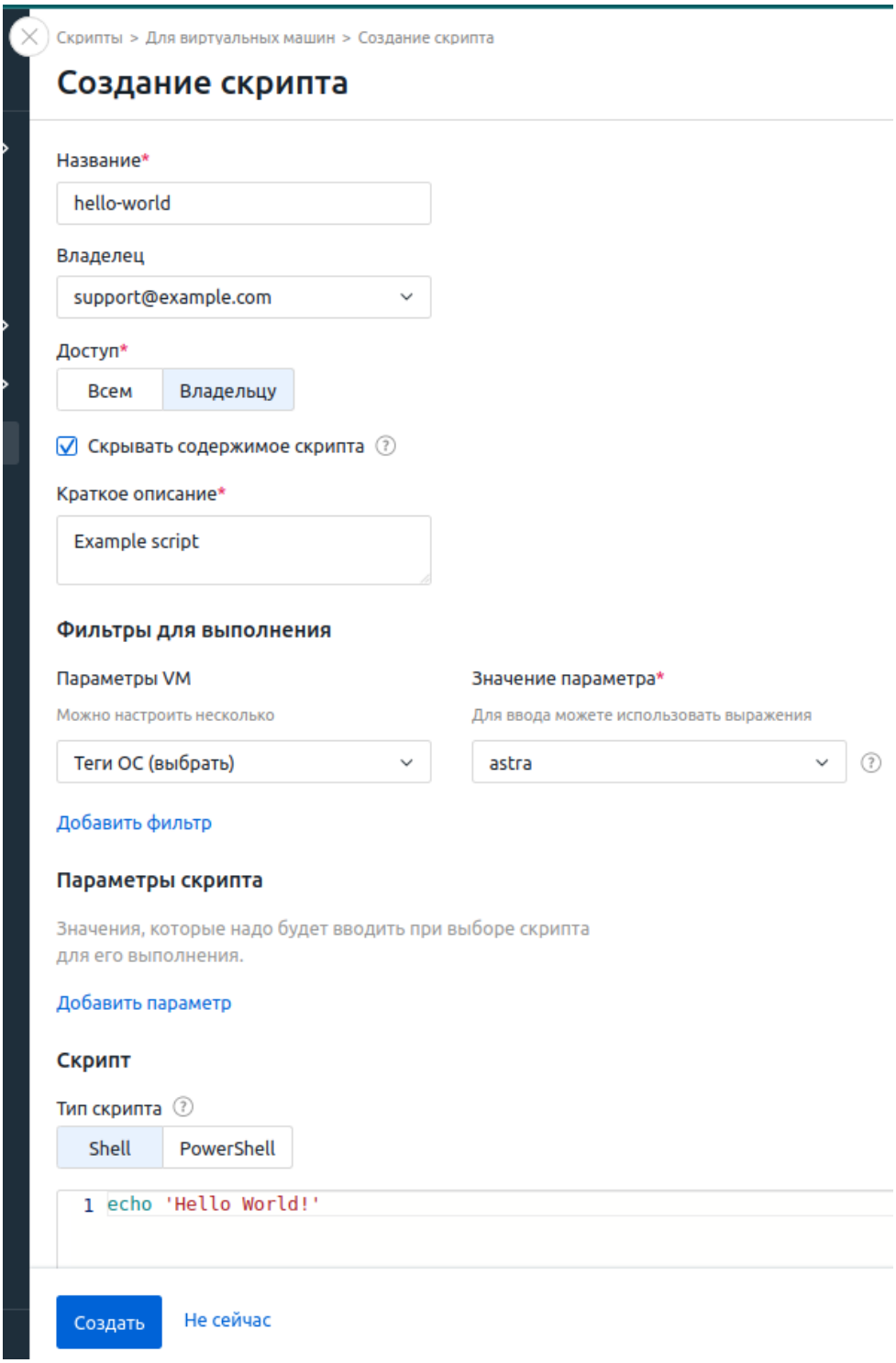

Рис. 29 — Создание скрипта

2.4.8.4. Резервное копирование ВМ

Резервная копия — это образ диска ВМ, который используется для ее восстановления. Возможно создание резервных копий вручную или по расписанию.

Порядок создания резервных копий вручную:

1) перейти в раздел «Виртуальные машины»;

2) выбрать ВМ, открыть меню «троеточие» и выбрать пункт «Создать резервную копию»;

3) выбрать диск, для которого нужно создать копию;

4) выбрать хранилище для копии — внешнее хранилище или узел, на котором находится ВМ. Чтобы VMmanager создал копию ВМ в самом свободном хранилище, выбрать пункт «Выбирать автоматически»;

5) ввести название новой копии;

6) ввести произвольное примечание;

7) нажать кнопку **[Создать резервную копию]**.

Пример создания резервной копии приведен на рис. 30.

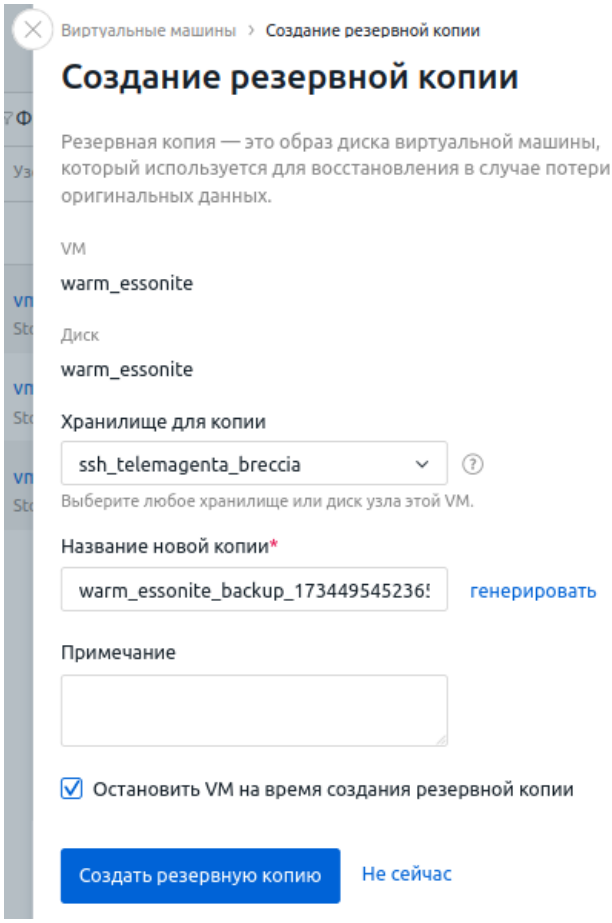

Рис. 30 — Создание резервной копии

Пример создания расписания резервного копирования приведен на рис. 31.

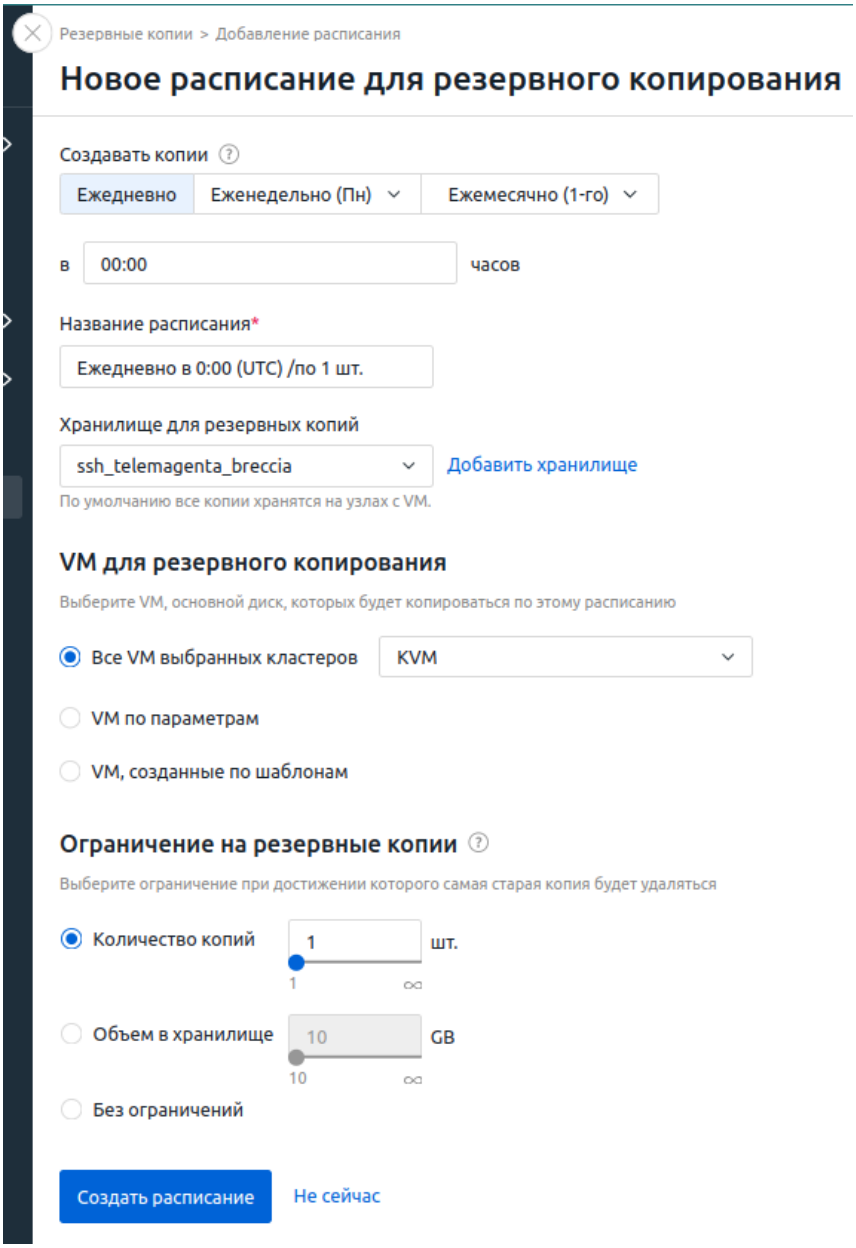

Рис. 31 — Создание расписания резервного копирования

Порядок создания расписания резервного копирования:

1) перейти в раздел «Резервные копии — Созданные по расписанию»;
2) нажать кнопку **[Создать расписание]**;
3) выбрать периодичность создания резервных копий:
   - «Ежедневно»;
   - «Еженедельно» — требуется выбрать день недели;
   - «Ежемесячно» — требуется выбрать число месяца;
4) ввести время в UTC, после которого VMmanager запустит создание копий;
5) ввести название расписания;
6) выбрать хранилище для резервных копий. Если выбрать несколько хранилищ, то VMmanager будет создавать резервные копии в самом свободном.

Если хранилище не выбрано, копия будет создана на узле кластера с исходной ВМ;

7) выбрать ВМ, которые будут копироваться по этому расписанию:
   - опция «Все VM выбранных кластеров» — требуется выбрать кластеры;
   - опция «VM по параметрам» — требуется выбрать ВМ;
   - опция «VM, созданные по шаблонам» — требуется выбрать конфигурацию ВМ;
8) установить одно из ограничений на резервные копии, при достижении которого самая старая копия каждой ВМ будет удаляться:
   - «Количество копий для каждой ВМ»;
   - «Объем в хранилище, занимаемый копиями каждой ВМ»;
   - «Без ограничений»;
9) нажать кнопку **[Создать расписание]**.

2.4.8.5. Перемещение (миграция) ВМ

Миграция — это перенос ВМ на другой узел. VMmanager позволяет выполнять миграцию ВМ как внутри одного кластера, так и в другой кластер.

Существует два типа миграции:

- без остановки ВМ (живая миграция) — ВМ остается доступной во время миграции;
- с остановкой ВМ — ВМ недоступна на время миграции.

Пример миграции ВМ приведен на рис. 32.

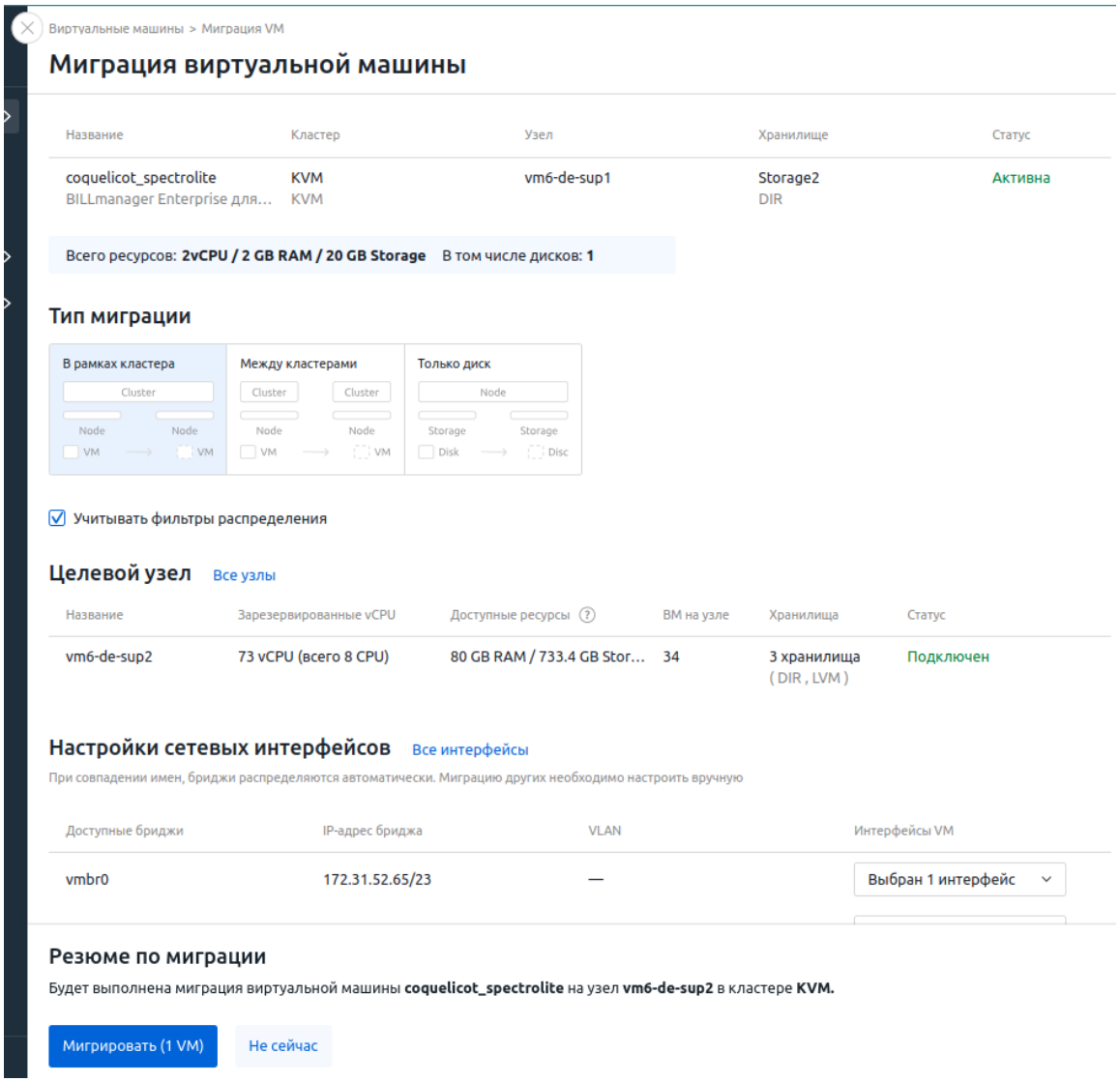

Рис. 32 — Миграция ВМ

Порядок запуска миграции:

1) перейти в раздел «Виртуальные машины»;

2) выбрать нужную ВМ, открыть меню «троеточие» и выбрать пункт «Мигрировать»;

3) выбрать тип миграции:

– опция «В рамках кластера» — ВМ останутся в том же кластере, но будут перенесены на другой узел;

– опция «Между кластерами» — ВМ будут перенесены в другой кластер;

– опция «Только диск» — диски ВМ будут перенесены в другое хранилище;

4) выбрать параметры миграции:

– снять опцию «Сжимать диск VM перед миграцией», если оптимизация диска не требуется;

– снять опцию «Учитывать фильтры распределения», если

использование фильтров не требуется;

– для миграции между кластерами в разделе «Целевой кластер» нажать кнопку **[Выбрать кластер]** и выбрать нужный кластер из списка;

– для миграции в рамках кластера или между кластерами в разделе «Целевой узел» нажать кнопку **[Выбрать узел]** и выбрать нужный узел из списка. Если узел недоступен, в столбце «Статус» отобразится причина его недоступности;

– в разделе «Настройки сетевых интерфейсов» выбрать какие интерфейсы на узле назначения будут соответствовать интерфейсам на исходном узле;

– в разделе «Распределение дисков VM» выбрать в каких хранилищах будут размещены диски ВМ. Диски одной ВМ могут быть размещены в разных хранилищах;

5) изучить информацию в разделе «Резюме по миграции». Раздел содержит информацию о том, все ли диски распределены и требуется ли для ВМ перезагрузка;

6) нажать кнопку **[Мигрировать]**.

2.4.8.6. Образы ВМ

Пользовательский образ — образ диска ВМ, который используется для создания новых ВМ.

Порядок создания образа:

1) перейти в раздел «Шаблоны — Образы VM»;

2) нажать кнопку **[Создать образ]**;

3) выбрать ВМ, чтобы создать копию ее диска. Название нового образа генерируется автоматически в формате: `<название ВМ>_<текущее время в UNIX-формате>`;

4) ввести произвольное примечание;

5) выбрать владельца образа;

6) выбрать, кому разрешен доступ к образу;

7) если из исходной ВМ не нужно удалять информацию, снять опцию «Обезличить образ»;

8) выбрать хранилище для образа;

9) нажать кнопку **[Создать]**.

Пример создания образа ВМ приведен на рис. 33.

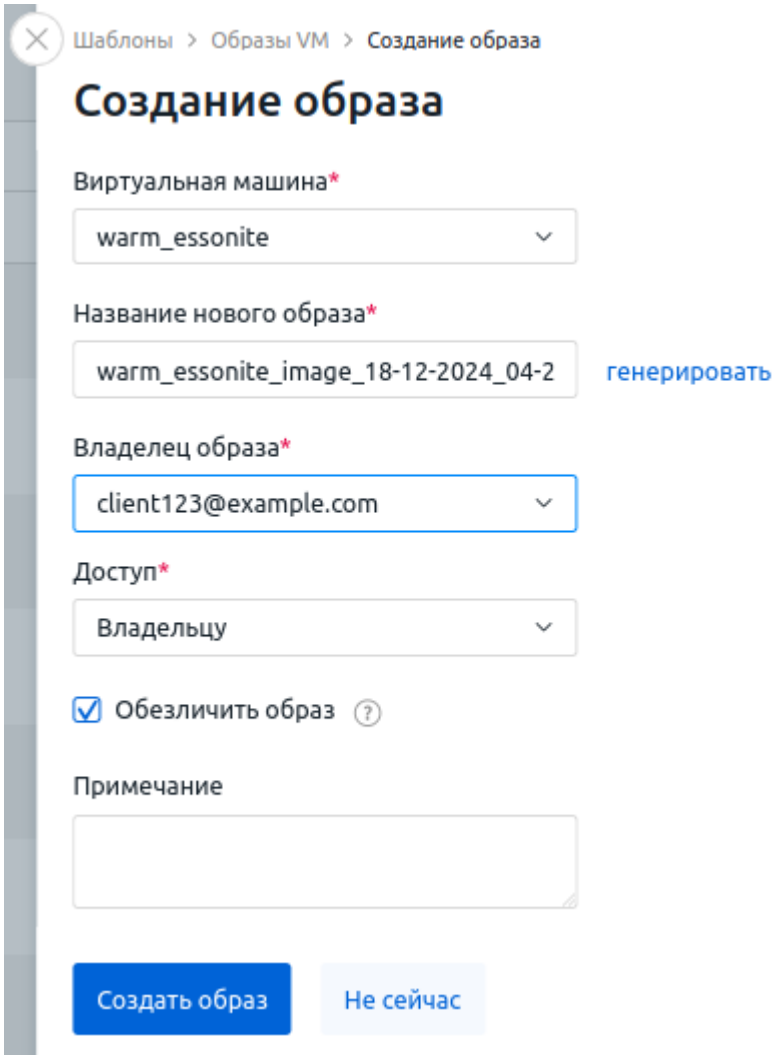

Рис. 33 — Создание образа ВМ

2.4.8.7. Клонирование ВМ

Клонирование — это создание копии ВМ. Для клонированной ВМ VMmanager:

- добавляет к имени префикс `_cloned`;
- генерирует новое доменное имя и MAC-адрес;
- выделяет новые IP-адреса из того же пула, что и у оригинальной ВМ;
- сохраняет все остальные настройки, включая владельца и пароль;
- устанавливает статус «Остановлена».

Порядок клонирования ВМ:

1) перейти в раздел «Виртуальные машины»;
2) выбрать ВМ, открыть меню «троеточие» и выбрать пункт «Клонировать».

2.4.8.8. Переустановка ОС на ВМ

Порядок переустановки ОС на ВМ:

1) перейти в раздел «Виртуальные машины»;

2) выбрать ВМ, открыть меню «троеточие» и выбрать пункт «Переустановить ОС»;

3) выбрать ОС для установки;

4) если требуется, выбрать скрипт для запуска после установки ОС;

5) ввести или сгенерировать новый пароль для доступа к ВМ;

6) нажать кнопку **[Переустановить]**.

Пример переустановки ОС приведен на рис. 34.

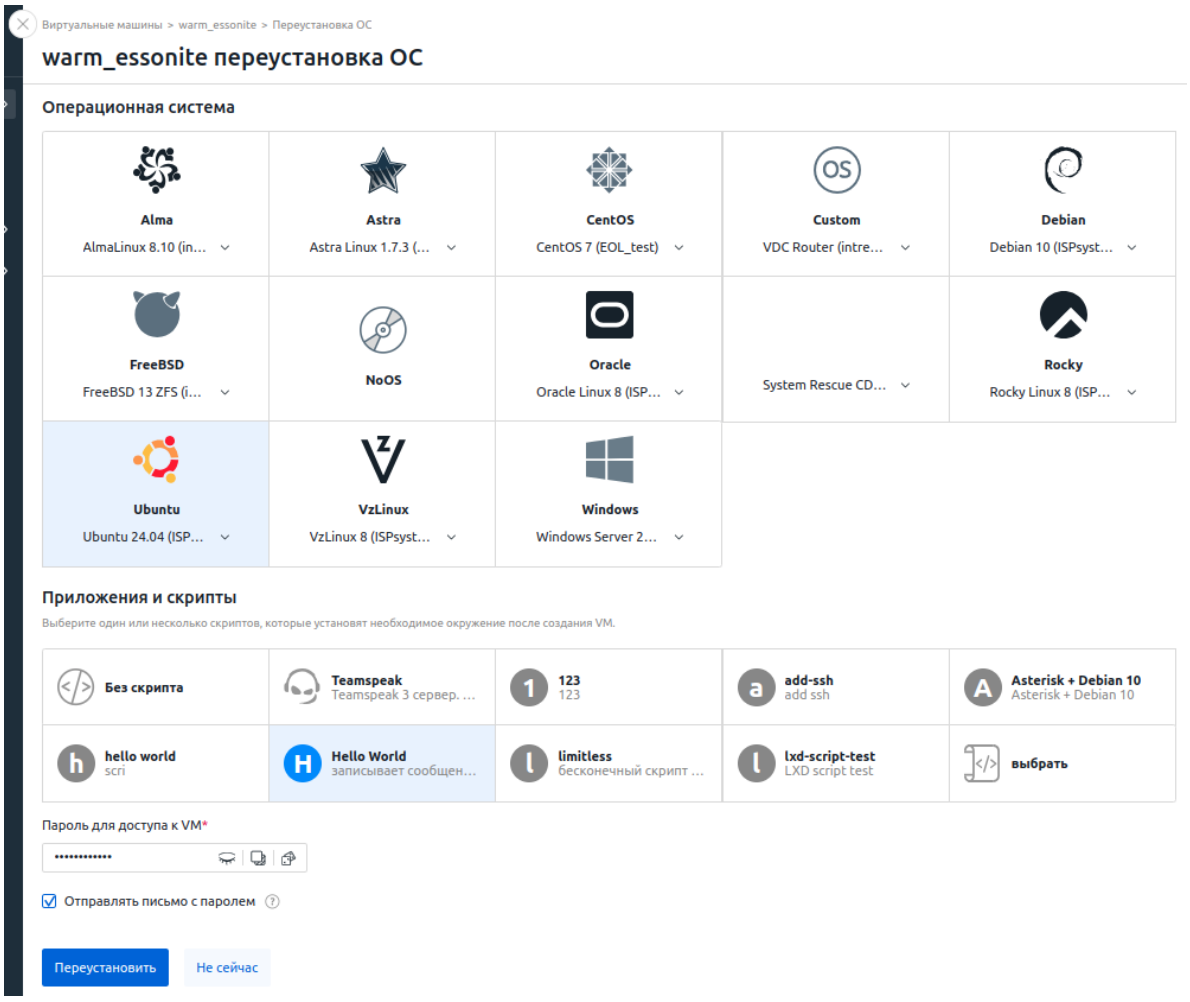

Рис. 34 — Переустановка ОС

2.4.8.9. Настройка подключения по VNC

VNC — система удаленного доступа к рабочему столу компьютера. VNC позволяет передавать нажатия клавиш на клавиатуре и движения мыши с одного компьютера на другой, ретранслировать содержимое экрана через компьютерную сеть.

VMmanager использует VNC для удаленного управления ВМ.

Порядок настройки подключения по VNC:

1) перейти в раздел «Виртуальные машины»;

2) выбрать ВМ и нажать кнопку **[Параметры]**;

3) перейти на вкладку «Настройка VNC/SPICE»;

4) ввести новый пароль для подключения;

5) нажать кнопку **[Сохранить и перезагрузить]**.

Пример настройки подключения по VNC приведен на рис. 35.

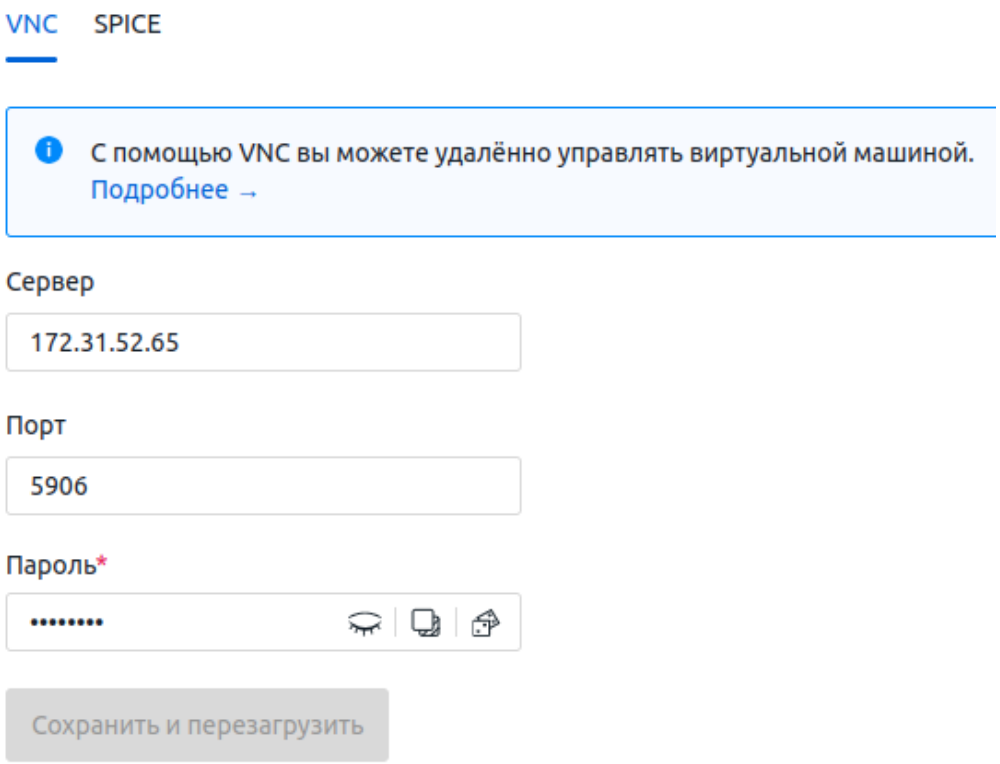

Рис. 35 — Настройки подключения по VNC

2.4.8.10. Настройка подключения по SPICE

SPICE — это протокол для удаленного подключения и управления ВМ. SPICE позволяет:

- автоматически изменять разрешение ВМ под размер экрана;
- настроить вывод ВМ на несколько дисплеев;
- подключать к ВМ USB-устройства;
- передавать буфер обмена;
- передавать файлы методом drag-and-drop.

Возможность подключения к ВМ по SPICE должна быть задана и в настройках кластера, и в настройках самой ВМ.

Чтобы разрешить подключения по SPICE на уровне кластера, необходимо установить опцию «Разрешить подключения по протоколу SPICE» в настройках кластера. При включении опции платформа добавит порты SPICE в правила файрвола на узлах кластера. Доступ по SPICE появится только у новых ВМ, которые будут созданы после

включения опции.

Чтобы разрешить доступ по SPICE к существующей ВМ:

1) перейти в раздел «Виртуальные машины»;
2) выбрать ВМ и нажать кнопку **[Параметры]**;
3) перейти на вкладку «Настройка VNC/SPICE — SPICE»;
4) установить опцию «Разрешить подключения по протоколу SPICE»;
5) нажать кнопку **[Сохранить и перезагрузить]**. Для применения настроек ВМ будет перезагружена.

Пример настройки подключения по SPICE приведен на рис. 36.

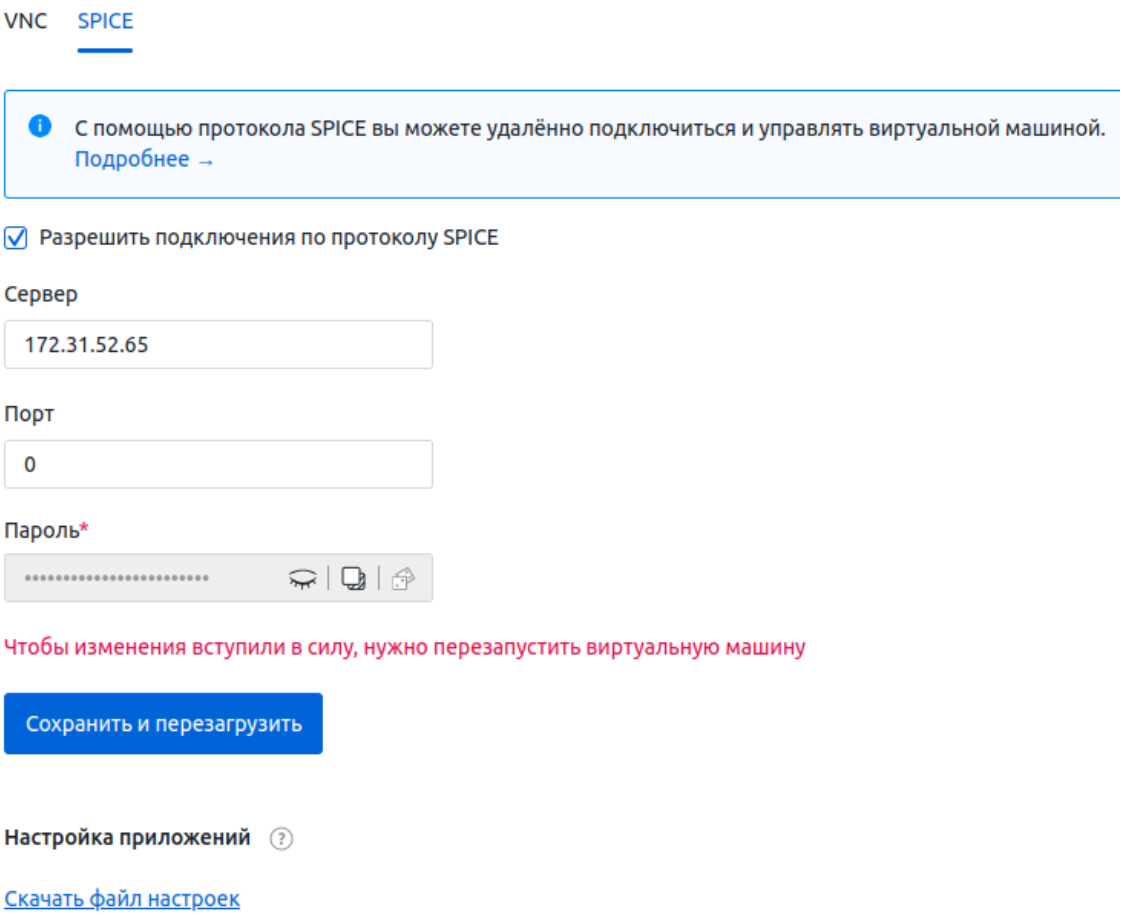

Рис. 36 — Настройки подключения по SPICE

2.4.8.11. Управление снимками состояния ВМ

Снимки состояния (снапшоты) ВМ создаются для сохранения текущего состояния RAM и дисков ВМ перед выполнением каких-либо рискованных действий.

Порядок создания снимков:

1) перейти в раздел «Виртуальные машины»;
2) выбрать ВМ, открыть меню «троеточие» и выбрать пункт «Создать снимок»;
3) если требуется, изменить название снимка. По умолчанию имена снимков

содержат дату и время создания;

4) если нужно, установить опцию «Сохранить состояние RAM»;
5) ввести произвольное примечание;
6) нажать кнопку **[Сохранить]**.

Пример создания снимка ВМ приведен на рис. 37.

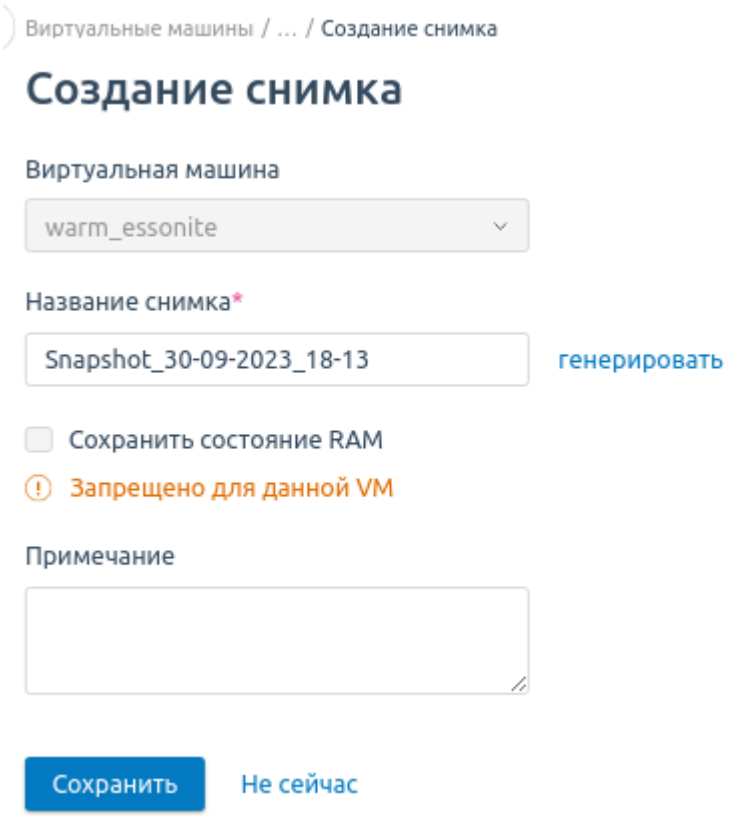

Рис. 37 — Создание снимка ВМ

2.4.8.12. Просмотр статистики ВМ

Порядок просмотра статистики ВМ:

1) перейти в раздел «Виртуальные машины»;
2) выбрать ВМ и нажать кнопку **[Параметры]**;
3) перейти на вкладку «Статистика»;
4) выбрать период просмотра статистики:
   - день;
   - неделя;
   - месяц;
   - год;
   - произвольный интервал дат.

Пример отображения статистики ВМ приведен на рис. 38.

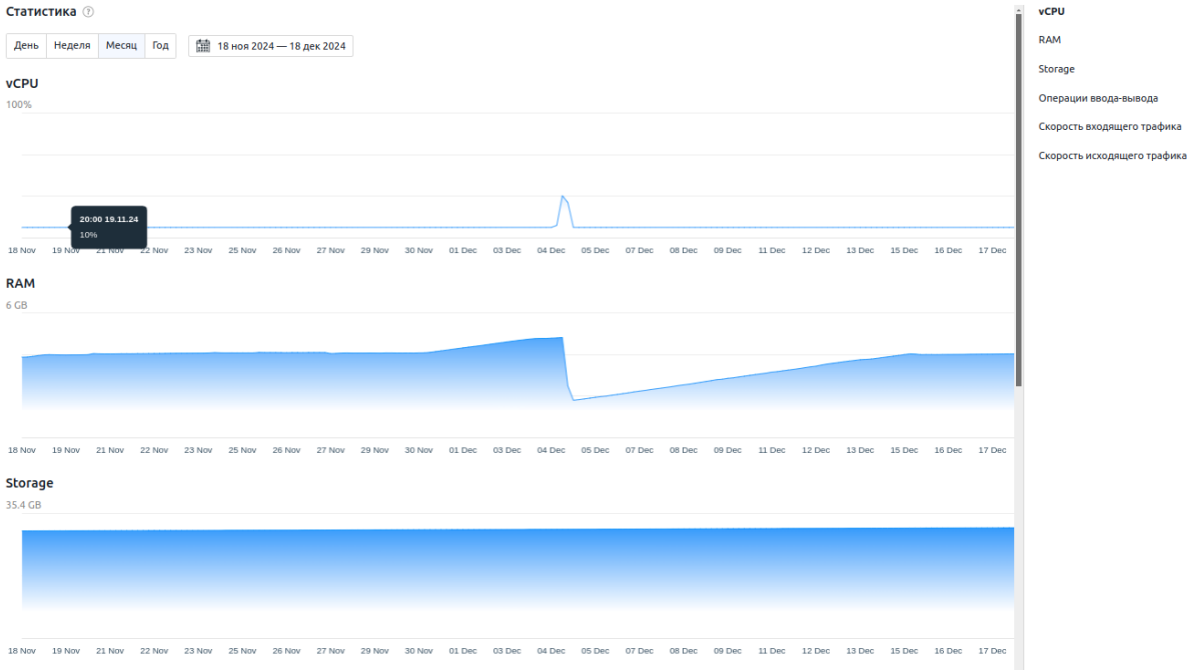

Рис. 38 — Отображение статистики ВМ

2.4.9. Настройка уведомлений

Уведомления — это сообщения для администраторов программы о состоянии ВМ и узлов кластера. Уведомления отображаются в интерфейсе программы и опционально дублируются на email администраторов и в мессенджер «Telegram».

Порядок настройки уведомлений:

1) нажать на значок «колокольчик» и выбрать пункт «Настройка уведомлений»;
2) нажать кнопку **[Настроить новое уведомление]**;
3) выбрать объекты, для которых требуется создать уведомления: «ВМ», «Узлы» или «Задачи»;
4) выбрать события для уведомлений;
5) выбрать email администраторов, на которые будут отправляться уведомления;
6) выбрать каналы «Telegram» для отправки уведомлений;
7) нажать кнопку **[Создать]**.

Пример настройки уведомлений приведен на рис. 39.

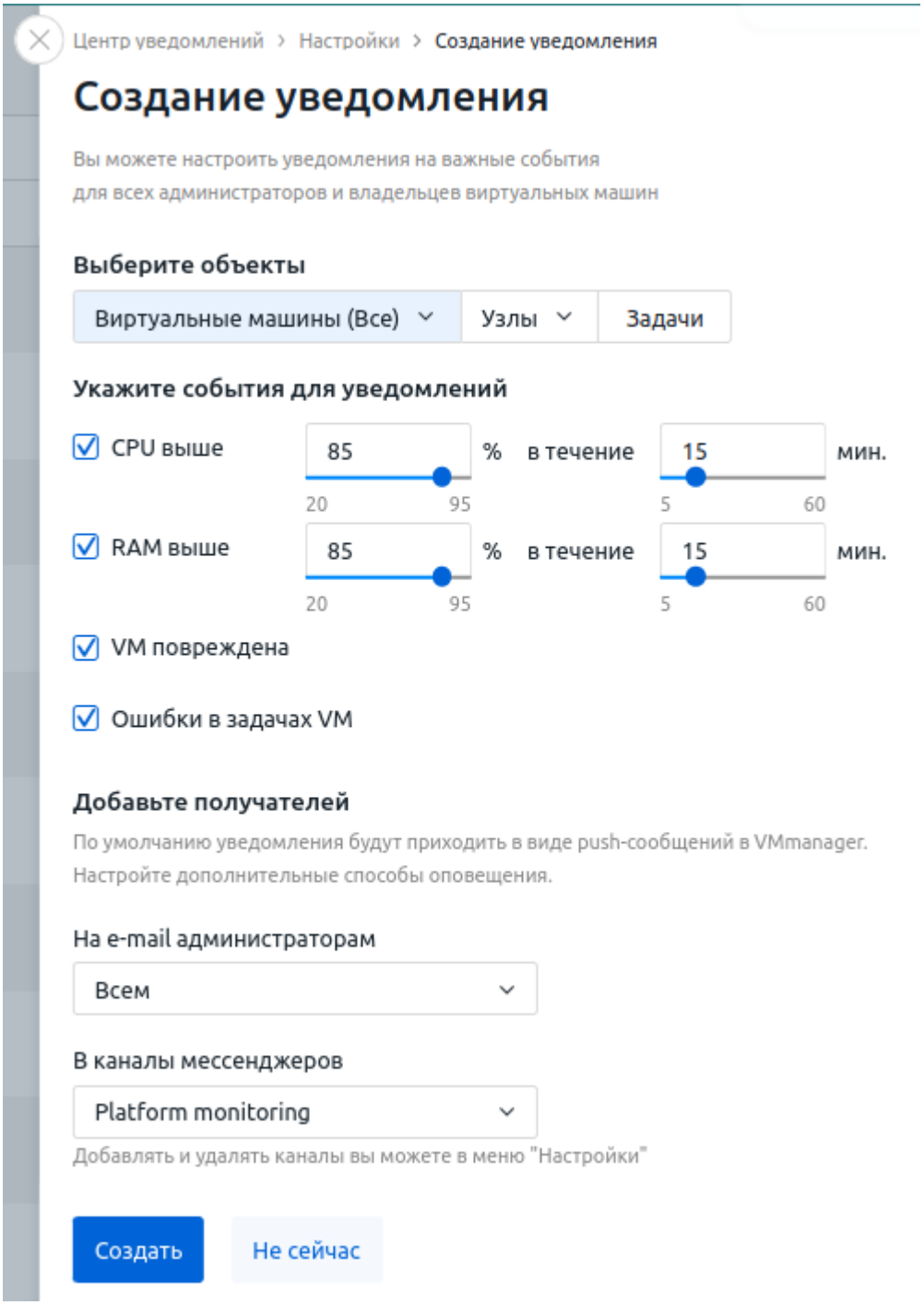

Рис. 39 — Настройка уведомлений

2.4.10. Настройки, доступные для администратора ВМ

Администратору ВМ доступно подключение к ВМ по протоколам VNC и SPICE.

2.4.10.1. Подключение к ВМ по протоколу VNC

Для подключения к ВМ по протоколу VNC через интерфейс платформы необходимо перейти в раздел «Виртуальные машины», выбрать ВМ, открыть меню «троеточие» и выбрать пункт «VNC». Рабочий стол ВМ откроется в отдельной вкладке браузера.

2.4.10.2. Подключение к ВМ по протоколу SPICE

Для подключения к ВМ по протоколу SPICE через интерфейс платформы необходимо перейти в раздел «Виртуальные машины», выбрать ВМ, открыть меню «троеточие» и выбрать пункт «SPICE». Рабочий стол ВМ откроется в отдельной вкладке браузера.

2.5. Проверка программы

Способы проверки работоспособности программы приведены в Таблице 3.

Таблица 3 — Способы проверки работоспособности программы

Испытание	Выполняемое действие	Критерий успешности
Установка программы	Инструкции из 2.4.1	ПО установлено, в настройках программы добавлен локальный репозиторий
Подключение SSL-сертификата	Инструкции из 2.4.3.1	Веб-интерфейс платформы открывается по протоколу HTTPS
Настройка почтового сервера	Инструкции из 2.4.3.2	На указанный email отправлено тестовое письмо
Настройка клиентского сервиса	Инструкции из 2.4.3.3	Заданные настройки отображаются в интерфейсе пользователя
Настройка отправки уведомлений в мессенджер «Telegram»	Инструкции из 2.4.3.4	В разделе «Настройки — Мессенджеры» отображается имя созданного бота и список каналов, доступных для уведомлений
Настройка резервного копирования платформы	Инструкции из 2.4.3.5	Резервные копии создаются согласно настройкам созданного расписания
Создание пользователей	Инструкции из 2.4.4.1	Созданный пользователь отображается в разделе «Пользователи». При приглашении пользователя на указанный email приходит письмо с приглашением
Создание групп пользователей	Инструкции из 2.4.4.2	Создана группа пользователей. При аутентификации пользователей группы с запрещенных IP-адресов в интерфейсе программы отображается ошибка
Синхронизация учетных записей с LDAP	Инструкции из 2.4.4.3	В программе созданы учетные записи из каталога LDAP

Продолжение таблицы 3

Испытание	Выполняемое действие	Критерий успешности
Создание физических сетей	Инструкции из 2.4.6.1	В разделе «Сети —Физические сети» добавлена физическая сеть с заданными параметрами
Создание пулов IP-адресов	Инструкции из 2.4.6.2	В разделе «Сети — Пулы IP-адресов» добавлен пул IP-адресов с заданными параметрами
Настройка DNSBL	Инструкции из 2.4.6.3	В разделе «Сети — DNSBL» добавлен список DNSBL с заданными параметрами
Создание кластера	Инструкции из 2.4.5.1	В программе создан кластер с заданными параметрами
Подключение узлов виртуализации	Инструкции из 2.4.5.2	В кластер добавлен узел виртуализации с заданными параметрами
Сетевые настройки узлов виртуализации	Инструкции из 2.4.5.3	На узле виртуализации созданы бридж и бонд с заданными параметрами
Настройка распределения ВМ	Инструкции из 2.4.5.4	Созданные ВМ размещаются на узлах виртуализации согласно заданным настройкам
Настройка отказоустойчивости	Инструкции из 2.4.5.6	В карточке кластера в разделе «Отказоустойчивость» отображаются заданные настройки
Настройка хранилищ кластера	Инструкции из 2.4.5.7	В карточке кластера в разделе «Локальные хранилища (Сетевые хранилища)» отображается информация о подключенном хранилище
Включение балансировщика	Инструкции из 2.4.5.8	В карточке кластера отображаются настройки балансировщика и индикаторы балансировки
Создание ВМ	Инструкции из 2.4.7.1	В разделе «Виртуальные машины» отображается информация о созданной ВМ
Настройка сети на ВМ	Инструкции из 2.4.8.1	На ВМ добавлены заданные IP-адреса
Управление дисками ВМ	Инструкции из 2.4.8.2	К ВМ добавлены диски с заданными параметрами

Продолжение таблицы 3

Испытание	Выполняемое действие	Критерий успешности
Запуск скриптов на ВМ	Инструкции из 2.4.8.3	В разделе «Скрипты» отображается информация о созданном скрипте
Резервное копирование ВМ	Инструкции из 2.4.8.4	В разделе «Резервные копии» карточки ВМ отображается информация о созданной копии. В разделе «Резервные копии — Созданные по расписанию» отображается информация о созданном расписании
Миграция ВМ	Инструкции из 2.4.8.5	ВМ перенесена на выбранный узел виртуализации
Создание образов ВМ	Инструкции из 2.4.8.6	В разделе «Шаблоны — Образы VM» отображается информация о созданном образе
Клонирование ВМ	Инструкции из 2.4.8.7	В разделе «Виртуальные машины» отображается информация о клоне ВМ
Переустановка ОС на ВМ	Инструкции из 2.4.8.8	В разделе «Информация» карточки ВМ отображается информация об установленной ОС
Настройка подключения по VNC	Инструкции из 2.4.8.9	При нажатии кнопки **[VNC]** в карточке ВМ выполняется подключение к ВМ по VNC
Настройка подключения по SPICE	Инструкции из 2.4.8.10	При нажатии кнопки **[SPICE]** в карточке ВМ выполняется подключение к ВМ по SPICE
Управление снимками ВМ	Инструкции из 2.4.8.11	В разделе «Снимки VM» карточки ВМ отображается информация о созданных снимках
Просмотр статистики ВМ	Инструкции из 2.4.8.12	В разделе «Статистика» карточки ВМ отображаются данные статистики ВМ
Настройка шаблонов ОС	Инструкции из 2.4.7.2	Настройки выбранного шаблона изменены
Настройка пользовательских образов ВМ	Инструкции из 2.4.7.3	Настройки выбранного образа изменены
Создание конфигурации ВМ	Инструкции из 2.4.7.4	В разделе «Шаблоны — Конфигурации VM» отображается информация о созданной конфигурации

Окончание таблицы 3

Испытание	Выполняемое действие	Критерий успешности
Добавление репозитория ОС	Инструкции из 2.4.7.1	В разделе «Шаблоны — Репозитории» отображается информация о созданном репозитории
Настройка уведомлений	Инструкции из 2.4.9	В разделе «Центр уведомлений» отображаются созданные настройки уведомлений

2.6. Сообщения системному программисту

Тексты сообщений, выводимых в ходе выполнения настройки, проверки программы и в ходе выполнения программы, описание их содержания и возможные действия приведены в Таблице 4.

Таблица 4 — Тексты сообщений и возможные действия

Внутренний идентификатор	Текст сообщения	Описание	Возможное действие
401	«Вы не авторизованы, или ваша сессия истекла, попробуйте повторно представиться системе»	Оператор не авторизован в программе	Повторить процедуру авторизации
403	«Нет хватает прав на совершение запроса»	У оператора отсутствуют права на выполнение запроса	Обратиться к администратору программы
404	«Запрашиваемая вами страница не найдена»	Запрос несуществующей страницы интерфейса	Вернуться на предыдущую страницу средствами браузера
501	«Произошла внутренняя ошибка сервера»	Внутренняя ошибка сервера	Выполнить запрос повторно
503	«Сервис временно недоступен. Попробуйте отправить запрос еще раз»	Проблема с работой сервиса	Выполнить запрос повторно
504	«Сервис не отвечает. Попробуйте отправить запрос позже»	Проблема с работой сервиса	Выполнить запрос повторно
3001	«Invalid login»	Неверный email и/или пароль учетной записи	Ввести корректный email и/или пароль

Продолжение таблицы 4

Внутренний идентификатор	Текст сообщения	Описание	Возможное действие
3005	«Access denied»	Доступ пользователя запрещен	Проверить настройки доступа для учетной записи
5006	«IP address unknown»	Указан несуществующий IP-адрес	Указать существующий IP-адрес
5007	«Cluster id unknown»	Указан несуществующий кластер	Указать существующий кластер
5008	«Mac id unknown»	Указан несуществующий MAC-адрес	Указать существующий MAC-адрес
5009	«Network id unknown»	Указана несуществующая сеть	Указать существующую сеть
5010	«Os id unknown»	Указан несуществующий шаблон ОС	Указать существующий шаблон ОС
5011	«Repository id unknown»	Указан несуществующий репозиторий	Указать существующий репозиторий
5012	«Disk id unknown»	Указан несуществующий диск	Указать существующий диск
5014	«Can not find proper task table record»	Не удается найти подходящую задачу в таблице задач	Уточнить условия поиска и повторить поиск задачи
5016	«Recipe id unknown»	Указан несуществующий скрипт для ВМ	Указать существующий скрипт
5017	«Preset id unknown»	Указана несуществующая конфигурация	Указать существующую конфигурацию
5018	«Network storage unknown»	Указано несуществующее сетевое хранилище	Указать существующее сетевое хранилище
5019	«Storage tag unknown»	Указан несуществующий тег хранилища	Указать существующий тег хранилища

Продолжение таблицы 4

Внутренний идентификатор	Текст сообщения	Описание	Возможное действие
5020	«Storage unknown»	Указано несуществующее локальное хранилище	Указать существующее локальное хранилище
5021	«Host id unknown»	Указана несуществующая ВМ	Указать существующую ВМ
5022	«Account id unknown»	Указана несуществующая учетная запись	Указать существующую учетную запись
5023	«Image id unknown»	Указан несуществующий образ	Указать существующий образ
5024	«Ip pool id unknown»	Указан несуществующий пул IP-адресов	Указать существующий пул IP-адресов
5025	«Node id unknown»	Указан несуществующий узел кластера	Указать существующий узел кластера
5026	«Ssh key id unknown»	Указан несуществующий SSH-ключ	Указать существующий SSH-ключ
5027	«Os Group unknown»	Указано несуществующее семейство ОС	Указать существующее семейство ОС
5028	«Hetzner ip id unknown»	Указан несуществующий IP-адрес в кластере с типом настроек «Маршрутизация»	Указать существующий IP-адрес
5029	«Hetzner subnet id unknown»	Указан несуществующая подсеть IP-адресов в кластере с типом настроек «Маршрутизация»	Указать существующую подсеть
5030	«Virt pool id unknown»	Указан несуществующий пул IP-адресов	Указать существующий пул
5031	«Inconsistent params of ippools connect»	Неверные параметры пула IP-адресов	Проверить параметры пула
5032	«Bad interface index»	Неверный индекс сетевого интерфейса	Проверить индекс сетевого интерфейса
5033	«Different number of interfaces»	Число сетевых интерфейсов отличается от требуемого	Проверить число сетевых интерфейсов

Продолжение таблицы 4

Внутренний идентификатор	Текст сообщения	Описание	Возможное действие
5034	«Must set interfaces»	Неверные параметры сетевых интерфейсов	Проверить параметры сетевых интерфейсов
5035	«Too many interfaces»	Число сетевых интерфейсов превышает максимально допустимое	Сократить число сетевых интерфейсов
5036	«Two interfaces no support ipv6»	Данная конфигурация не поддерживает IPv6-адресацию	Изменить конфигурацию или сменить тип адресации на IPv4
5037	«Host interface unknown»	Указан несуществующий интерфейс ВМ	Указать существующий интерфейс ВМ
5039	«Backup location unknown»	Указано несуществующее хранилище резервных копий ВМ	Указать существующее хранилище
5040	«Schedule unknown»	Указано несуществующее расписание резервного копирования ВМ	Указать существующее расписание
5041	«Platform backup schedule unknown»	Указано несуществующее расписание резервного копирования платформы	Указать существующее расписание
5042	«Platform backup storage unknown»	Указано несуществующее хранилище резервных копий платформы	Указать существующее хранилище
5043	«Platform backup unknown»	Указана несуществующая резервная копия платформы	Указать существующую копию
5046	«Storage to cluster unknown»	Указано несуществующее хранилище кластера	Указать существующее хранилище
5047	«Storage unknown»	Указано несуществующее хранилище	Указать существующее хранилище

Продолжение таблицы 4

Внутренний идентификатор	Текст сообщения	Описание	Возможное действие
5048	«Script variable unknown»	Указана несуществующая переменная скрипта	Указать существующую переменную
5049	«Recipe param unknown»	Указана несуществующий параметр скрипта	Указать существующий параметр
5050	«Ip network id unknown»	Указана несуществующиая физическая сеть	Указать существующую сеть
5052	«Host interface id unknown»	Указан несуществующий интерфейс ВМ	Указать существующий интерфейс
5053	«Node interface id unknown»	Указан несуществующий интерфейс узла виртуализации	Указать существующий интерфейс
5054	«Node bridge id unknown»	Указан несуществующий бридж	Указать существующий бридж
5055	«Node bond id unknown»	Указан несуществующий бонд	Указать существующий бонд
5056	«Ip pool to cluster unknown»	Указан несуществующий пул IP-адресов в кластере	Указать существующий пул
5058	«Can not find allocated ip in ipmgr»	Не найден IP-адрес	Проверить правильность IP-адреса
5059	«Disk bus is unknown»	Указан несуществующий тип подключения диска	Указать существующий тип подключения
5060	«IP address unknown»	Указан несуществующий IP-адрес	Указать существующий IP-адрес
5061	«Disk backup unknown»	Указана несуществующая резевная копия диска	Указать существующую копию
5063	«Snapshot id unknown»	Указана несуществующий снимок ВМ	Указать существующий снимок ВМ
5064	«Tag id unknown»	Указан несуществующий тег	Указать существующий тег

Продолжение таблицы 4

Внутренний идентификатор	Текст сообщения	Описание	Возможное действие
5065	«Preset disk id unknown»	Указана несуществующая конфигурация диска	Указать существующую конфигурацию
5072	«Live migration of VMs snapshots is not allowed»	Живая миграция недоступна для ВМ со снимками и дисками формата Qcow2	Удалить снимки ВМ или выполнить миграцию с остановкой ВМ
5100	«Некоторые IP-адреса заняты блоком»	Выбраны IP-адреса, пересекающиеся с существующим блоком	Изменить диапазон выбранных IP-адресов
5101	«Сеть пересекается с уже существующей»	Настройки создаваемой сети пересекаются с настройками существующей	Изменить настройки создаваемой сети
5102	«IP-адрес занят»	IP-адрес занят	Выбрать другой IP-адрес
5103	«Network cannot be deleted. There is a dependent IP»	Сеть не может быть удалена, так как есть зависимые IP-адреса	Определить зависимые IP-адреса и освободить их. Повторить удаление сети
5104	«Invalid IP»	Обращение к неправильному IP-адресу	Проверить настройки IP-адреса
5105	«Invalid IP range»	Обращение к неправильному диапазону IP-адресов	Проверить настройки диапазона IP-адресов
5106	«Node cannot be deleted. There is a dependent host»	Узел виртуализации не может быть удален, так как на нем располагаются ВМ	Удалить ВМ с узла виртуализации, повторить удаление узла
5107	«Cluster cannot be deleted. There is a dependent node»	Кластер не может быть удален, есть зависимые узлы	Удалить зависимые узлы виртуализации, повторить удаление кластера
5112	«Not enough rights on object»	Недостаточно прав для доступа к объекту	Проверить права доступа к объекту
5113	«There is no node in cluster»	Кластер не содержит ни одного узла	Добавить узел виртуализации в кластер
5114	«Cluster with same name already exists»	Кластер с указанным именем уже существует	Выбрать другое имя для кластера
5120	«Bad URL»	Неверный URL-адрес	Проверить правильность ввода URL

Продолжение таблицы 4

Внутренний идентификатор	Текст сообщения	Описание	Возможное действие
5121	«Source param missed»	Пропущен параметр для создания ВМ, нет ОС или образа	Проверить правильность указанных параметров
5123	«Cluster cannot be selected automatically»	Кластер не может быть выбран автоматически	Выбрать кластер вручную
5124	«OS not available on cluster»	ОС недоступна на текущем кластере	Выбрать другую ОС или другой кластер
5125	«Node check failed»	Проверка узла кластера завершилась с ошибкой	Проверить состояние сервера узла
5126	«Host creation blocked on node»	Создание ВМ на узле заблокировано	Разрешить создание ВМ на узле
5127	«Can't find source location»	Не удалось найти узел, содержащий образ	Проверить наличие необходимого образа на узлах
5128	«Node is not ready»	Узел не готов к работе	Проверить работосопособность узла
5129	«Image is not available»	Образ недоступен	Проверить состояние образа
5130	«Invalid time zone»	Неверная временная зона	Изменить временную зону
5131	«OS not available on node»	ОС недоступна на узле	Проверить наличие необходимой ОС на узле
5132	«Account cannot be deleted. There is a dependent host»	Учетная запись не может быть удалена, есть зависимые VM	Удалить зависимые ВМ, повторить удаление учетной записи
5134	«There is no suitable node in cluster»	В выбранном кластере нет подходящего по параметрам узла.	Выбрать другой кластер
5137	«Cluster doesn't have any pools»	К кластеру не подключены пулы IP-адресов	Подключить пул IP-адресов к кластеру
5138	«Selected pools are not connected to the cluster»	Выбранные пулы IP-адресов не подключены к кластеру	Подключить пулы IP-адресов к кластеру
5140	«Some ips from this subnet are used in vm»	Подсеть содержит занятые IP-адреса	Выбрать другую подсеть
5141	«Ip is active»	IP-адрес используется на ВМ	Выбрать другой IP-адрес

Продолжение таблицы 4

Внутренний идентификатор	Текст сообщения	Описание	Возможное действие
5145	«Minimal prefix in hetzner datacenter is 24»	Минимальный префикс для типа сетевых настроек «Маршрутизация» - «24».	Увеличить значение префикса
5146	«Bad ipv6 subnet prefix»	Значение префикса для IPv6 не поддерживается	Указать значение префикса от «32» до «96»
5147	«No connected IPv6 subnet on node»	На узле виртуализации нет IPv6-подсетей	Создать IPv6-подсеть
5148	«Not enough free IPv6 blocks on the node»	Нет свободных блоков IPv6 на узле	Освободить используемый блок IPv6-адресов
5149	«Invalid ssh key»	Неверный SSH-ключ	Проверить корректность SSH-ключа
5151	«No disk found for host»	Не найден диск для ВМ	Проверить правильность указания диска
5152	«No interface found for host»	Не найден интерфейс для ВМ	Проверить правильность указания интерфейса
5153	«ISO count limit exceeded»	Количество ISO-образов превышено	Удалить часть ISO-образов
5154	«ISO size is too big»	Размер ISO-образа превышает максимально допустимый	Изменить параметр "Макс.размер загружаемых ISO" в разделе настроек системы
5155	«ISO is already mounted to host»	К ВМ уже подключен ISO-образ	Отключить подключенный ISO-образ
5156	«ISO check is failed»	ISO-образ не прошел проверку	Проверить целостность ISO-образа
5159	«Backup location check failed»	Не удалось проверить хранилище резервных копий	Проверить доступ к хранилищу
5160	«Operation is not allowed for remotely stored images»	Операция не поддерживается для образов, хранящихся удаленно	Выбрать образ в локальном хранилище
5162	«Backup storage connection check failed»	Проверка подключения хранилища резервных копий не удалась	Проверить доступ к хранилищу

Продолжение таблицы 4

Внутренний идентификатор	Текст сообщения	Описание	Возможное действие
5163	«Platform backup schedule have no connected storage»	В расписании резервного копирования платформы не выбрано хранилище	Выбрать хранилище в настройках расписания
5164	«Failed to open platform backup file»	Не удалось открыть файл с резервной копией платформы	Проверить наличие и целостность файла, при необходимости выбрать другой файл, повторить операцию
5165	«Failed to start platform backup process»	Не удалось запустить восстановление платформы из резервной копии	Проверить наличие и целостность файла, при необходимости выбрать другой файл, повторить операцию
5166	«Bad cron expression»	Ошибка в записи cron	Проверить формат записи cron в настройках расписания
5169	«CPU cores number on node exceeds license limit»	Количество ядер CPU для ВМ на узле превышает лимит	Увеличить доступное число vCPU в настройках узла
5170	«VM per node limit exceeded»	Количество ВМ на узле превышает лимит	Увеличить доступное число ВМ в настройках узла
5171	«Live migration from newer to older libvirt version not allowed»	Живая миграция с данными версиями libvirt не поддерживается	Выполнить миграцию с остановкой ВМ
5172	«Host is still creating»	ВМ еще создается	Дождаться создания ВМ
5173	«Host is in relocation failed state»	ВМ еще мигрирует	Дождаться окончания миграции ВМ
5174	«Bridge already paired with the host interface»	ВМ уже подключена к выбранному бриджу	Выбрать другой бридж
5178	«Node network settings already locked»	Сетевая конфигурация узла заблокирована для изменений	Дождаться изменения конфигурации узла
5179	«Iface/Bond can't be paired widh more than one Vlanless bridge»	Интерфейс может быть подключен только к одному бриджу без VLAN	Отключить интерфейс от подключенного бриджа и повторить подключение к необходимому бриджу

Продолжение таблицы 4

Внутренний идентификатор	Текст сообщения	Описание	Возможное действие
5181	«Node already have default bridge»	Бридж по умолчанию уже существует	Снять опцию «Сделать бриджем по умолчанию для создания VM» у бриджа по умолчанию и установить ее для нужного бриджа
5182	«Invalid slave interface for bridge»	Выбранный интерфейс не может быть включен в бридж	Выбрать другой интерфейс
5183	«Interface already included to another bond/bridge»	Выбранный интерфейс уже включен в бонд или бридж	Отключить интерфейс от бонда/бриджа или выбрать другой интерфейс
5184	«Cannot remove the default node bridge»	Невозможно удалить бридж по умолчанию	Отключить опцию «Сделать бриджем по умолчанию для создания VM» у бриджа по умолчанию
5185	«Some iface/bond/bridge has already used this name»	Выбранное имя интерфейса уже используется	Выбрать другое имя интерфейса
5190	«Bridge/Bond name matches a reserved pattern»	Данное имя интерфейса зарезервировано и не может быть использовано	Выбрать другое имя интерфейса
5195	«Cluster doesn't have any pools»	К кластеру не подключены пулы IP-адресов	Подключить пулы к кластеру
5197	«IP is already allocated in panel»	IP-адрес зарезервирован	Выбрать другой IP-адрес
5198	«IP address not found»	IP-адрес не найден	Проверить правильность выбора IP-адреса
5203	«Specified disk is not linked with the specified host»	Выбранный диск не подключен к выбранной ВМ	Подключить диск к ВМ
5206	«Disk limit for the specified bus type has been reached»	Превышено количество дисков для выбранного типа подключения	Выбрать другой тип подключения
5207	«Cannot unlink last host disk»	Невозможно отключить единственный диск от ВМ	Подключить дополнительный диск, сделать его основным и отключить нужный диск

Продолжение таблицы 4

Внутренний идентификатор	Текст сообщения	Описание	Возможное действие
5209	«Specified host is not on the specified node»	Нельзя изменить префикс блока IPv6-адресов, выделяемых для VM, есть используемые IPv6-адреса	Освободить занятые IPv6-адреса
5210	«Cannot remove disk which linked to host»	Невозможно отключить диск, не подключенный к ВМ	Проверить правильность выбора диска
5211	«Cannot unlink main host disk»	Невозможно отключить основной диск от ВМ	Подключить дополнительный диск, сделать его основным и отключить нужный диск
5212	«Disk already linked with host»	Диск уже подключен к ВМ	Проверить правильность выбора диска
5213	«Blocked for host with mounted ISO»	Недоступно для ВМ с подключенным ISO-образом	Отключить ISO-образ
5214	«Host and disk have to locate on the same node»	ВМ и диск должны находиться на одном узле	Выбрать один узел для ВМ и диска
5215	«Disk and host have to belong the same account»	У ВМ и диска должен быть один владелец	Выбрать одного владельца для ВМ и диска
5216	«Linked disk cannot migrate between nodes»	Подключенный диск не может быть мигрирован между узлами	Отключить диск от ВМ
5217	«Migration destination is equal to source»	Узел назначения совпадает с исходным узлом	Выбрать другой узел назначения
5218	«Node has dependent host backups»	У узла есть зависимые резервные копии ВМ	Удалить зависимые резервные копии
5219	«Node already exists»	Узел с таким именем уже существует	Выбрать другое имя узла
5221	«Node cannot be deleted. There is a dependent disk»	Узел не может быть удален, т.к. есть зависимый диск	Удалить зависимый диск
5224	«Suitable storage is not found»	Не найдено подходящее хранилище	Проверить состояние хранилищ, при необходимости подключить дополнительное хранилище

Продолжение таблицы 4

Внутренний идентификатор	Текст сообщения	Описание	Возможное действие
5225	«Can not migrate between clusters with different datacenter type»	Невозможно мигрировать ВМ между кластерами с разными типами настройки сети	Выбрать кластер с идентичным типом настройки сети
5231	«Several interfaces are not supported for the datacenter with the routing network model»	Для типа сетевых настроек «Маршрутизация» не поддерживаются узлы с двумя интерфейсами	Использовать один интерфейс узла при подключении
5302	«Invalid network mask»	Неверная сетевая маска	Проверить правильность ввода сетевой маски
5303	«No suitable network»	Нет подходящей сети	Добавить сеть с нужными параметрами
5305	«IP busy»	IP-адрес занят	Выбрать другой IP-адрес
5306	«Not enough free IP in selected pools»	Нет свободных адресов	Добавить пул IP-адресов
5308	«License expired»	Лицензия истекла	Продлить срок лицензии
5309	«Empty license»	Отсутствуют данные о лицензии	Проверить состояние лицензии
5310	«Invalid license»	Данные о лицензии повреждены	Повторно выполнить активацию лицензии
5314	«Image Limit Exceeded»	Достигнут лимит по количеству образов	Удалить неиспользуемые образы
5315	«License file expired»	Данные о лицензии просрочены	Проверить состояние лицензии
5320	«New disk size incorrect»	Некорректный новый размер диска	Указать корректный размер диска
5321	«Not enough free disk space in storage»	Недостаточно свободного места в хранилище	Освободить место на диске хранилища или удалить неиспользуемые ВМ
5322	«Image limit exceeded for host»	Превышено количество доступных образов для данной ВМ	Удалить неиспользуемые образы
5330	«Host is crashed»	VM повреждена	Запустить ВМ в режиме восстановления, выполнить действия по восстановлению

Продолжение таблицы 4

Внутренний идентификатор	Текст сообщения	Описание	Возможное действие
5339	«Ippool has used IP»	Невозможно удалить пул, есть используемые IP-адреса	Освободить используемые IP-адреса
5342	«Empty params for run recipe»	Пустые параметры для запуска скрипта	Указать необходимые параметры для запуска
5343	«Not enough CPU in node»	Недостаточно CPU на узле	Сократить количество vCPU, потребляемых ВМ, или удалить неиспользуемые ВМ
5344	«Not enough free RAM in node»	Недостаточно RAM на узле	Сократить объем RAM в ресурсах для ВМ, удалить неиспользуемые VM или увеличить объем RAM на узле
5345	«The network exists but the gateway does not match»	Сеть существует, но шлюз не совпадает	Указать корректный шлюз для сети
5349	«Can not connect with node»	Нет соединения с узлом виртуализации	Проверить доступ к узлу виртуализации с сервера платформы
5350	«Could not delete running task»	Только отложенные задачи или находящиеся в очереди могут быть удалены	Дождаться выполнения задачи
5352	«No KVM virtualization support on node»	Отсутствует аппаратная поддержка виртуализации	Проверить настройки виртуализации в BIOS/UEFI узла виртуализации, проверить поддержку виртуализации для процессора командой: `grep -P 'vmx|svm' /proc/cpuinfo`
5353	«KVM virtualization support is disabled in BIOS settings»	Аппаратная поддержка виртуализации отключена в BIOS	Проверить настройки виртуализации в BIOS/UEFI узла виртуализации
5354	«Can not get node info»	Невозможно получить информацию об узле виртуализации	Проверить доступ к узлу виртуализации с сервера платформы
5355	«Such a hostname is already used for another node in the cluster»	Узел с данным именем уже существует	Выбрать другое имя узла

Продолжение таблицы 4

Внутренний идентификатор	Текст сообщения	Описание	Возможное действие
5356	«Can not migrate hosts from different clusters»	Групповая миграция для ВМ из разных кластеров не возможна	Выполнить миграцию ВМ из каждого кластера поочередно
5359	«Can not add the node with active SELinux»	Невозможно подключить узел, на котором работает SELinux	Отключить службу SELinux на узле виртуализации, повторить добавление узла
5360	«Can not add the node with SELinux enabled in /etc/selinux/config»	Невозможно подключить узел, на котором не отключен SELinux в файле `/etc/selinux/config`	Отключить службу SELinux в файле `/etc/selinux/config` на узле виртуализации, повторить добавление узла
5362	«Disk too small for selected OS»	Задан недостаточный размер диска ВМ для выбранной ОС	Увеличить размер диска ВМ
5363	«Disk too small for selected image»	Задан недостаточный размер диска ВМ для выбранного образа ВМ	Увеличить размер диска ВМ
5364	«No email params in license»	Лицензия не содержит информации о настройках электронной почты по умолчанию	Проверить состояние лицензии
5366	«Connection timeout»	Не удалось подключиться к узлу	Проверить доступ к узлу виртуализации с сервера платформы
5371	«VM is in rescue mode»	ВМ находится в режиме восстановления	Отключить режим восстановления
5375	«Week day is not set for weekly schedule»	Не выбран день недели для запуска расписания	Выбрать день недели
5376	«Month day is not set for monthly schedule»	Не выбрано число месяца для запуска расписания	Выбрать число месяца
5377	«Hosts or clusters are not set for schedule»	Не выбраны ВМ и/или кластеры в расписании	Выбрать ВМ и/или кластеры
5366	«Connection timeout»	Не удалось подключиться к узлу	Проверить доступ к узлу виртуализации с сервера платформы

Продолжение таблицы 4

Внутренний идентификатор	Текст сообщения	Описание	Возможное действие
5371	«VM is in rescue mode»	ВМ находится в режиме восстановления	Отключить режим восстановления
5378	«Start time is not set for schedule»	Не выбрано время запуска в расписании	Выбрать время запуска
5379	«VM is unavailable»	ВМ недоступна	Проверить состояние ВМ
5382	«vCPU number is not set»	Количество vCPU не задано	Указать количество vCPU
5383	«RAM is not set»	Объем RAM не задан	Указать объем RAM
5384	«Disk size is not set»	Размер диска не задан	Указать объем диска
5389	«Invalid resource value»	Некорректное значение ресурса	Указать корректное значение
5391	«Recipe param must have a value»	Не задано значение для параметра скрипта	Указать значение параметра
5392	«Unsupported preset of vm on cluster»	Неподдерживаемая конфигурация ВМ в кластере	Выбрать поддерживаемую конфигурацию
5394	«No recipient were provided»	Не указан получатель уведомления о выполнении скрипта	Указать получателя уведомления
5395	«Recipient doesn't have language»	Не указан язык получателя уведомления о выполнении скрипта	Указать язык получателя
5396	«Recipient doesn't have email»	Не указан email получателя уведомления о выполнении скрипта	Указать email получателя
5397	«No template was found for specified language»	Для выбранного языка нет шаблона уведомления о выполнении скрипта	Выбрать другой язык или создать шаблон
5403	«LVM is not tuned»	ПО для работы с LVM не установлено	Установить ПО LVM в хранилище кластера
5404	«LVM volume group is not set»	Группа томов LVM не найдена	Создать группу томов в настройках ПО LVM
5405	«Not found suitable LVM volume group in several VGs»	Не найдено группы томов с подходящим именем	Укажите для одной из групп томов имя, соответствующее настройках хранилища

Продолжение таблицы 4

Внутренний идентификатор	Текст сообщения	Описание	Возможное действие
5406	«Not found LVM volume group with suitable name»	Не найдено группы томов с подходящим именем	Укажите для одной из групп томов имя, соответствующее настройках хранилища
5408	«Vm storage path not set»	Путь к хранилищу ВМ не найден	Уточните путь к хранилищу
5409	«Volume group name not set»	Группа томов не задана	Задайте группу томов в настройках кластера
5410	«OS storage path not set»	Хранилище для шаблонов ОС не задано	Указать хранилище для шаблонов ОС
5504	«Cpu overselling set lower then 0.5. Try to increase overselling over 0.5»	Оверселлинг CPU ниже допустимого	Установите значение оверселлинга не менее 0,5
5904	«Main storage not found on cluster»	Основное хранилище не подключено к кластеру	Выбрать одно из хранилищ в качестве основного
5906	«Storage not found on destination node»	На узле назначения не найдены хранилища	Выбрать другой узел назначения
5907	«VM storage path is a required parameter for File storage»	Для файлового хранилища необходимо указать директорию хранения ВМ	Указать директорию хранения ВМ
5908	«Volume group is a required parameter for LVM storage»	Для LVM необходимо указать группу томов	Указать группу томов
5910	«RBD pool name is a required parameter for Ceph storage»	Для Ceph необходимо указать имя пула RBD	Указать имя пула RBD
5911	«RBD user is a required parameter for Ceph storage»	Для Ceph необходимо указать пользователя RBD	Указать пользователя RBD
5912	«Storage params is a required parameter for Ceph storage»	Для Ceph необходимо указать настройки хранилища	Указать настройки хранилища
5913	«IP address is a required parameter for Ceph storage»	Для Ceph необходимо указать IP-адрес	Указать IP-адрес хранилища
5914	«SSH port is a required parameter for Ceph storage»	Для Ceph необходимо указать SSH-порт	Указать SSH-порт хранилища

Продолжение таблицы 4

Внутренний идентификатор	Текст сообщения	Описание	Возможное действие
5915	«Storage is disabled on cluster»	Хранилище отключено в кластере	Включить хранилище
5916	«Main storage is disabled on cluster»	Основное хранилище отключено в кластере	Включить основное хранилище
5918	«Cluster does not has storages»	К кластеру не подключены хранилища	Подключить хранилища к кластеру
5920	«Storage with same params is already attached to cluster»	Хранилище с такими параметрами уже подключено к кластеру	Проверить параметры подключаемого хранилища
5921	«Storage on destination node is not active»	Хранилище на узле назначения отключено	Включить хранилище на узле назначения
5922	«Neither ceph nor cephadm utils are not found on the server»	В хранилище Ceph не установлено необходимое ПО	Установить необходимое ПО и выполнить настройку хранилища
5923	«Repository with the same name already exists»	Репозиторий с таким именем уже существует	Изменить имя подключаемого репозитория
5924	«Repository with the same URL already exists»	Репозиторий с таким URL уже существует	Изменить URL подключаемого репозитория
5925	«Failed to get repository metadata»	Не удалось получить метаданные репозитория	Проверить корректность и доступность метаданных в репозитории
5926	«Repository metadata validation failed»	Метаданные репозитория некорректны	Проверить корректность метаданных в репозитории
5931	«Disk path is a required parameter for Network LVM storage»	Для сетевого LVM требуется указать путь к диску	Указать путь к диску
5933	«Storage does not support HA cluster»	Выбранный тип хранилища не поддерживается в HA-кластере	Выбрать поддерживаемый тип хранилища
5936	«HA is disabled on cluster»	Отказоустойчивость в кластере отключена	Включить отказоустойчивость в настройках кластера
5943	«Range contains in network with empty gateway»	Не указан шлюз для диапазона IP-адресов	Указать шлюз
5944	«IP-pool contains network with empty gateway»	Не указан шлюз для пула IP-адресов	Указать шлюз

Продолжение таблицы 4

Внутренний идентификатор	Текст сообщения	Описание	Возможное действие
5945	«Default bridge on node not found»	Бридж по умолчанию не найден	Назначить один из интерфейсов бриджем по умолчанию
5958	«License token not found»	Токен лицензии не найден	Повторно активировать лицензию
5959	«Update license failed»	Обновление лицензии не удалось	Проверить статус лицензии, повторно активировать лицензию
5960	«Activate license packet failed»	Активация пакета лицензии не удалась	Проверить статус пакета лицензии, повторно активировать пакет
5963	«License packet is already activated. If activated license packet is not listed in settings, try to update license»	Пакет лицензии уже активирован	Повторно активировать лицензию, проверить статус пакета, повторно активировать пакет
5964	«Cannot find node with matching host filter params»	Не удалось найти узел с подходящими параметрами фильтров	Измените параметры фильтров
5972	«Portstart is greater than portend»	Начальный порт диапазона больше конечного	Изменить настройки диапазона портов
5973	«Filter expression validation failed»	Значение фильтра задано некорректно	Указать корректное значение фильтра
5975	«Host params doesn't match with recipe filters»	Параметры ВМ не соответствуют заданному фильтру	Изменить условия фильтра
5992	«Qemu guest agent is not available on host»	На ВМ не установлен QEMU Guest Agent	Установить ПО QEMU Guest Agent на ВМ
5997	«ISO check timeout is exceeded»	Превышено время проверки ISO-образа	Проверить целостность файла образа, повторить загрузку
6001	«SPICE is disabled on cluster»	SPICE отключен в кластере	Разрешить подключения по SPICE в настройках кластера
6002	«SPICE is failed on node»	Не удалось включить SPICE на узле виртуализации	Проверить состояние узла
6005	«SPICE is disabled on host»	SPICE отключен на ВМ	Разрешить подключения по SPICE в настройках ВМ

Окончание таблицы 4

Внутренний идентификатор	Текст сообщения	Описание	Возможное действие
6022	«Only NAS storage is supported for current operation»	Операция будет доступна только при выборе NAS-хранилища	Выбрать для операции NAS-хранилище
6023	«Only local storage is supported for current operation»	Копирование и миграция недоступны для образа, созданного в NAS-хранилище	Выбрать локальное хранилище для копирования или миграции
6024	«Only same NAS storage is supported for current operation»	Операция будет доступна только при выборе NAS-хранилища, в котором был создан образ ВМ.	Выбрать NAS-хранилище с образом ВМ
6026	«Nas storage path is a required parameter for Nas storage»	Не указан параметр «Путь до директории на узлах».	Указать значение параметра
6027	«EFI boot can be set only for NoOS»	Загрузчик ОС не может быть запущен	Создать ВМ без ОС для запуска загрузчика
6029	«Only unique NAS storage path can use»	Значение поля «Путь до директории на узлах» должно быть уникальным	Указать уникальное значение параметра
6052	«Unsupported linked-clone main disk storage type»	Неподдерживаемый тип хранилища для операции со связанным клоном	Выбрать файловое или NAS-хранилище
6054	«The image is used by linked-clone»	Невозможно удалить образ ВМ из-за созданных связанных клонов	Удалить связанные клоны, созданные на основе этого образа, и повторить операцию
6056	«Linked-clone inter cluster migration not available»	Миграция связанных клонов между кластерами запрещена	Выполнить миграцию без смены кластера

3. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

3.1. Действия по приемке поставленного средства

При приемке экземпляра Изделия в поставке по сетям связи необходимо провести следующие проверки:

- проверка электронной подписи изготовителя образа с установочным диском изделия и формуляра в формате PDF;
- проверка комплектности в соответствии с формуляром;
- проверка маркировки – наличия в разделе 8 формуляра уникального идентификатора ФСТЭК России;
- проверка контрольной суммы образа установочного диска.

Контроль целостности образов контейнеров из состава установочного диска подтверждается средствами контроля целостности (средствами контроля соответствия дистрибутиву) путем вычисления и сравнения контрольных сумм исполняемых файлов и библиотек с эталонными значениями, хранящимися в файле `vm6.checksum`, входящем в состав установочного диска и обновления изделия.

Проверка контрольных сумм исполняемых файлов и библиотек изделия после установки на средство вычислительной техники осуществляется в соответствии с 3.2.4.

3.2. Действия по безопасной установке и настройке средства

3.2.1. Действия при установке ОС на мастер-сервере и узлах виртуализации

VMmanager функционирует в среде Astra Linux (очередное обновление 1.8) на усиленном уровне защищенности (режим «Воронеж»).

Для обеспечения корректного функционирования VMmanager необходимо, чтобы было установлено ПО оперативного обновления Astra Linux бюллетень № 2024-0905SE18 (оперативное обновление 1.8.1.uu1) или более поздних версий, при условии наличия сведений о совместимости и возможности установки на официальном информационном ресурсе: `https://ispsystem.ru/docs/vmmanager-gost`.

Рекомендуется применение ядра linux-6.6-generic.

При установке Astra Linux:

1) обязательными к установке являются компоненты:
   - «Средства виртуализации»;
   - «Консольные утилиты»;
   - «Средства удаленного подключения SSH»;
   - «Графический интерфейс Fly»;
2) на этапе «Дополнительные настройки ОС» должны быть отключены опции:

- «Запрет установки бита исполнения»;
- «Запрет исполнения скриптов пользователя».

Включение опции «Замкнутая программная среда» возможно после успешной установки платформы.

3.2.2. Действия после установки ОС на мастер-сервере

Администратор для безопасной установки и настройки средства должен:

1) перейти в режим суперпользователя командой: `sudo su -`

2) настроить список источников в файле `/etc/apt/sources.list` — убедиться, что в источниках в файле `/etc/apt/sources.list` закомментированы все, кроме `deb cdrom`;

3) изменить настройки сетевого интерфейса сервера: назначить статический IP и указать DNS, используя консольную утилиту `nmcli`. Вариант листинга команд для `nmcli`:

получить название соединения, на котором будем изменять IP:

```
nmcli c s
nmcli c m uuid <UUID соединения из вывода команды выше - можно использовать табуляцию> ipv4.method manual ipv4.addresses <Ваш IP/маска> ipv4.dns <Ваш DNS>
sudo nmcli device reapply <Ваш интерфейс - можно использовать табуляцию>
```

Пример применения команд на рис. 40:

Рис. 40 — Команды настройки сетевого интерфейса

4) создать файл `/etc/resolv.conf` и указать в нем настройки DNS-серверов;

5) перезапустить сервис networking командой: `service networking restart`

3.2.3. Действия после установки ОС на узлах виртуализации

Администратор для безопасной установки и настройки средства на серверах с Astra Linux в режиме защищенности «Воронеж» должен:

1) отключить службы astra-sudo-control, astra-nochmodx-lock, astra-interpreters-lock командами:

- `astra-sudo-control disable`

- `astra-nochmodx-lock disable`
- `astra-interpreters-lock disable`

2) создать директорию для ВМ (например, /vm) и установить для нее мандатные атрибуты командой:

`sudo mkdir <имя_директории> && sudo pdpl-file 0:63:0:ccnr <имя_директории>`

3) добавить в файл `/home/<имя_пользователя>/.ssh/authorized_keys` публичный SSH-ключ мастер-сервера;

4) установить права для файла `/home/<имя_пользователя>/.ssh/authorized_keys` командами:

- `chmod 600 /home/<имя_пользователя>/.ssh/authorized_keys`
- `chown <имя_пользователя> /home/<имя_пользователя>/.ssh/authorized_keys`

5) добавить в файл `/etc/ssh/sshd_config` строку `PermitRootLogin prohibit-password`;

6) в файле `/etc/sudoers` разрешить выполнение команд от имени суперпользователя командами через добавление строк:

- `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`
- `%sudo ALL=(ALL:ALL) NOPASSWD: ALL`

7) перезапустить сервис sshd командой:

`service sshd restart`

8) после добавления узла виртуализации в платформу выполнить команды:

- `usermod -G astra-admin -a <имя_пользователя>`
- `pdpl-user -i 63 <имя_пользователя>`

3.2.4. Проверка контрольных сумм исполняемых файлов и библиотек

Чтобы обеспечить контроль целостности средства, администратору необходимо выполнить проверку контрольных сумм исполняемых файлов и библиотек, входящих в состав средства. Проверка осуществляется с помощью скрипта `vm6_check_checksum.sh` и файла `vm6.checksum`, входящих в состав эксплуатационной документации изделия. При проверке скрипт сравнивает контрольные суммы файлов с данными из файла vm6.checksum и в случае несовпадения выводит сообщение об ошибке. Порядок проверки:

1) скопировать файлы `vm6_check_checksum.sh` и `vm6.checksum` в директорию `/opt/ispsystem/vm/` мастер-сервера;

2) запустить скрипт командой:

```
sh vm6_check_checksum.sh
```

3) изучить вывод скрипта:

– в случае совпадения контрольных сумм скрипт выведет сообщения вида «`Checking <имя_контейнера> ... Ok`»;

– в случае несовпадения контрольной суммы контейнера скрипт выведет сообщение вида «`Checking <имя_контейнера> ... Container SHA mismatch`»;

– в случае несовпадения контрольной суммы файлов скрипт выведет сообщение «`Checking <имя_контейнера> ... sha256sum: WARNING: <количество_файлов> computed checksum did NOT match`» с указанием имен файлов.

3.3. Действия по реализации функций безопасности среды функционирования средства

Администратор для реализации функций безопасности среды функционирования средства должен:

1) выполнить действия по настройке ЗПС на мастер-сервере и узлах виртуализации:

– если режим ЗПС не был включен при установке ОС, включить его командой:

```
sudo astra-digsig-control enable
```

– скачать открытый ключ разрабочика изделия для ЗПС командой:

```
wget https://download.ispsystem.com/6/astra_se/exo-soft_pub.key -O /etc/digsig/keys/exo-soft_pub.key
```

– инициализировать ключ для всех ядер центрального процессора командой:

```
sudo update-initramfs -u -k all
```

– перезагрузить сервер;

2) выполнить настройку сетевого оборудования для работы в замкнутой программной среде;

3) провести контроль целостности файлов ВМ, создаваемых ПО libvirt;

4) настроить требуемый уровень логирования для регистрации событий безопасности;

5) настроить синхронизацию программы с каталогом LDAP.

В целях обеспечения удаленного доступа пользователей с использованием сетей связи общего пользования к средству виртуализации должны применяться средства криптографической защиты информации, прошедшие процедуру оценки соответствия в соответствии с законодательством Российской Федерации.

4. РУКОВОДСТВО АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

Данный раздел предназначен для пользователей, для которых назначена роль в VMmanager — Администратор безопасности. Учетная запись администратора безопасности в ОС должна входить в группу пользователей astra-audit.

4.1. Регистрация событий безопасности в VMmanager

В VMmanager регистрация событий безопасности выполняется с учетом требований ГОСТ Р 59548-2022.

Регистрация событий безопасности реализуется использованием службы auditd и подсистемы регистрации событий из состава Astra Linux. Служба auditd выполняет регистрацию событий объектов файловой системы (аудит файлов) и пользователей (аудит процессов) согласно заданным правилам. Регистрация событий осуществляется в журнал аудита.

Описание настройки параметров регистрации событий безопасности приведено в документе РУСБ.10015-01 97 01-1.

4.2. Настройка регистрации событий безопасности

Для настройки регистрации событий безопасности используется программа fly-admin-events из состава Astra Linux, с помощью которой доступно выполнять регистрацию событий запуска и остановки службы auditd, регистрацию событий добавления и удаления правил auditd, регистрацию действий с журналом аудита. Дополнительно утилита позволяет добавлять правила аудита. Порядок использования программы fly-admin-events приведен в электронной справке.

Кроме того, для управления правилами аудита используются следующие инструменты командной строки из состава Astra Linux:

- getfaud — служит для получения списков правил регистрации событий над файловыми объектами;
- setfaud — устанавливает на файлы списки правил регистрации событий;
- useraud — позволяет просматривать и изменять правила регистрации событий для пользователей;
- psaud — позволяет изменить или считать правила регистрации событий заданного процесса;
- ausearch — предназначен для просмотра файлов журнала регистрации событий ядра, а также событий пользователя.

Описание представленных выше инструментов командной строки приведено в документе РУСБ.10015-01 97 01-1.

4.3. Журнал событий

Служба syslog-ng выполняет регистрацию событий в журнал `/parsec/log/astra/events`. В журнале событий регистрируются попытки запуска неподписанных файлов, успешная и неуспешная авторизация, данные о пользовательских сессиях и другие события безопасности, регистрация которых настроена.

Для просмотра журнала событий может использоваться:

– программа fly-event-viewer («Журнал системных событий»), описание программы приведено в электронной справке. Программа fly-event-viewer устанавливается вместе с компонентом ОС «Графический интерфейс Fly»;

– инструмент командной строки astra-event-viewer, порядок использования инструмента приведен на странице помощи, вызываемой командой: `astra-event-viewer -h`

Действия с журналом событий (удаление, переименование, перемещение, ротация файла журнала событий) регистрируются подсистемой регистрации событий и указываются первой записью в журнале событий:

– удаление журнала событий регистрируется событием «Журнал событий удален»;

– переименование или перемещение журнала событий регистрируется событием «Журнал событий переименован или перемещен»;

– ротация журнала событий регистрируется событием «Журнал событий ротирован»;

– действия с журналом событий недоверенными процессами (всеми процессами, кроме процессов syslog-ng и logrotate) регистрируются событием «Журнал событий изменен недоверенным процессом».

Кроме того, программа fly-event-viewer позволяет выполнить выгрузку (экспорт) данных из журнала событий безопасности в файл формата CSV или JSON. Порядок действий описан в электронной справке.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ВМ	–	Виртуальная машина
ЕПП	–	Единое пространство пользователей
ЗПС	–	Замкнутая программная среда
МКЦ	–	Мандатный контроль целостности
ОС	–	Операционная система
ПО	–	Программное обеспечение
BIOS	–	Базовая система ввода-вывода (Basic Input/Output System)
CPU	–	Центральный процессор (Central Prosessing Unit)
DNS	–	Система доменных имен (Domain Name System)
DN	–	Отличительное имя (Distinguished Name)
DNSBL	–	«Черные списки» доменов и IP-адресов (DNS Blocklist)
DS	–	Распределенный коммутатор (Distributed Switch)
FTP	–	Протокол передачи файлов (File Transfer Protocol)
HA	–	Высокая доступность (High Availability)
HTTPS	–	Протокол передачи гипертекста с поддержкой шифрования (Hypertext Transfer Protocol Secure)
ID	–	Идентификатор (Identifier)
IDE	–	Параллельный интерфейс подключения накопителей (Integrated Drive Electronics)
IP	–	Интернет-протокол (Internet Protocol)
ISO	–	Образ оптического диска
IPv4	–	Четвертая версия интернет-протокола (Internet Protocol version 4)
IPv6	–	Шестая версия интернет-протокола (Internet Protocol version 6)
KVM	–	ПО, обеспечивающее аппаратную виртуализацию (Kernel-based Virtual Machine)
LDAP	–	Протокол быстрого доступа к каталогам (Lightweight Directory Access Protocol)
LVM	–	Менеджер логических томов (Logical Volume Manager)
NAS	–	Сервер хранения данных на уровне файлов (Network Attached Storage)
OS	–	Операционная система (Operating System)

QEMU	–	Программа для эмуляции аппаратного обеспечения (Quick Emulator)
RAM	–	Оперативная память (Random-Access Memory)
RBD	–	Блочное устройство хранилища Ceph (RADOS Bloack Device)
RHEL	–	Дистрибутив Linux компании Red Hat (Red Hat Enterprise Linux)
RSA	–	Криптографический алгоритм с открытым ключом (Rivest–Shamir–Adleman)
SAN	–	Сеть хранения данных (Storage Area Network)
SASL	–	Фреймворк для аутентификации и защиты данных в протоколах на основе соединений (Simple Authentication and Security Layer)
SCSI	–	Набор стандартов для физического подключения и передачи данных между компьютерами и периферийными устройствами (Small Computer System Interface)
SMTP	–	Сетевой протокол для передачи сообщений электронной почты (Simple Mail Transfer Protocol)
SPICE	–	Протокол для удаленного подключения и управления ВМ (Simple Protocol for Independent Computing Environments)
SSH	–	Протокол для безопасной работы с сетевыми сервисами (Secure Shell)
SSL	–	Протокол для создания зашифрованного соединения с веб-сервером (Secure Sockets Layer)
TLS	–	Протокол защиты транспортного уровня (Transport Layer Security)
UEFI	–	Интерфейс взаимодействия между ОС и микропрограммами (Unified Extensible Firmware Interface)
URL	–	Унифицированный указатель ресурса (Uniform Resource Locator)
UTC	–	Всемирное координированное время (Coordinated Universal Time)
vCPU	–	Виртуальный центральный процессор (virtual Central Processing Unit)
VM	–	Виртуальная машина (Virtual Machine)

VNC	–	Система удаленного доступа к рабочему столу виртуальной машины (Virtual Network Computing)

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопрово-дитель-ного документа и дата	Подпись	Дата
	изме-ненных	заме-ненных	новых	аннули-рованных					
1		Все					НЦСВ.02-24 от 16.10.2024		
2		Все					НЦСВ.01-25 от 03.03.2025		