

Д. С. Андрианова ¹

¹РГУ нефти и газа (НИУ) имени И.М. Губкина, г. Москва, Российская Федерация

МИГРАЦИЯ ВИРТУАЛЬНЫХ МАШИН С VIRTUAL APPLIANCE (OVA) НА ZVIRT. ВОПРОСЫ НАДЁЖНОСТИ, БЕЗОПАСНОСТИ

Аннотация: В статье рассматривается миграция виртуальных машин из формата Virtual Appliance (OVA), применяемого в гипервизорах VMware и VirtualBox, на отечественную платформу виртуализации zVirt версии 4.5. Актуальность исследования обусловлена необходимостью импортозамещения зарубежных средств виртуализации, а также обеспечением надёжности и безопасности при переносе виртуальной инфраструктуры. Цель работы заключается в экспериментальной проверке возможности холодной миграции виртуальной машины в среду zVirt 4.5 с сохранением её работоспособности и основных параметров безопасности.

В ходе исследования был разработан и развёрнут экспериментальный стенд, включающий хост виртуализации, NFS-хранилище и менеджер управления. На стенде была выполнена миграция виртуальной машины под управлением операционной системы Microsoft Windows 10 из OVA-формата в среду zVirt. Особое внимание уделено конвертации виртуального диска из формата VMDK в целевой формат, корректности импорта, сохранению сетевых параметров и проверке функционирования виртуальной машины после переноса.

По результатам эксперимента подтверждена возможность успешной холодной миграции виртуальной машины на платформу zVirt 4.5. Для оценки надёжности и безопасности были выполнены сравнение хеш-сумм исходного и перенесённого OVA-образа, анализ журналов событий, а также проверка сохранения прав доступа NTFS/ACL. Полученные результаты показывают, что при корректной подготовке инфраструктуры миграция может быть выполнена с сохранением целостности данных, работоспособности виртуальной машины и контролируемости процесса переноса.

Ключевые слова: zVirt, Virtual Appliance, OVA, хеш-сумма, надёжность, безопасность, миграция.

Введение

В современном мире миграция виртуальных машин (далее – ВМ) играет ключевую роль в обеспечении гибкости и масштабируемости информационных технологий. Миграция представляет собой перенос виртуальных машин с исходного узла на целевой. Она применяется для балансировки нагрузки между серверами, проведения технического обслуживания без остановки сервисов, аварийного восстановления при сбоях, а также для переноса ВМ между различными платформами виртуализации в целях импортозамещения.

Актуальность исследования обусловлена необходимостью внедрения и обеспечения надёжности и безопасности миграции ВМ средствами отечественного программного продукта для виртуализации и управления виртуальной инфраструктурой zVirt версии 4.5. Это позволит повысить безопасность, надёжность и управляемость ВМ, с учётом современных требований к платформам виртуализации и отечественному программному обеспечению.

Проблема, решаемая в данной работе, заключается в отсутствии экспериментальных исследований, верифицирующих процедуру холодной миграции виртуальных машин из формата Virtual Appliance (OVA) на отечественную платформу виртуализации zVirt 4.5, учитывая обеспечение критериев безопасности и надёжности. Анализ существующих публикаций показывает, что основное внимание уделяется либо теоретическим аспектам миграции виртуальных машин на отечественную платформу zVirt 4.5, либо настройке на зарубежном оборудовании (Proxmox, Hyper-V) [1–2].

Целью работы является исследование и экспериментальная реализация миграции виртуальной машины с Virtual Appliance (OVA) на отечественную платформу виртуализации zVirt 4.5 с учётом требований к надёжности и безопасности.

Объектом исследования выступает процесс миграции виртуальной машины с Virtual Appliance (OVA) на отечественную платформу виртуализации zVirt 4.5.

Предметом исследования являются методы и процедуры настройки, реализации и обеспечения безопасности и надёжности миграции из Virtual Appliance (OVA) в среду

Рубрика 2. Методы и системы защиты информации, информационная безопасность

программного обеспечения zVirt 4.5. В рамках работы изучаются особенности настройки параметров виртуальной инфраструктуры, а также вопросы надёжности и безопасности.

Метод основан на экспериментальном подходе и сравнительном анализе полученных результатов с критериями надёжности и безопасности.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Провести анализ предметной области миграции ВМ из формата Virtual Appliance (OVA) и его особенности на основе современных подходов к виртуализации, требований к безопасности и надёжности.
2. Проанализировать особенности формата Virtual Appliance (OVA).
3. Спроектировать и развернуть экспериментальный стенд, имитирующий инфраструктуру миграции на основе программного решения zVirt 4.5.
4. Обеспечить надёжность и безопасность процесса миграции и эксплуатации ВМ.
5. Провести тестирование корректности работы виртуальной машины после миграции на платформу zVirt 4.5.

Литературный обзор

Проблема, рассматриваемая в работе Л.Е. Попок [3], заключается в недостаточной работоспособности комплексных методик миграции виртуальных машин с платформы VMware vSphere на Microsoft Hyper-V. Автор рассматривает подходы к конвертации виртуальных машин между гипервизорами VMware и Hyper-V, а также совместимость дисков (VMDK в VHDX). Однако Л.Е. Попок не рассматривает реализацию миграции виртуальных машин на отечественных платформах виртуализации.

Работа Цыганковой А.А. и Климченко К.П. [4] посвящена сравнительному анализу отечественных платформ виртуализации Брест и zVirt, проведённому на основе критериев, важных для дальнейшего внедрения в образовательный процесс. Однако данные исследования носят теоретический характер и не затрагивают практическую реализацию и тестирование на отечественных платформах виртуализации.

В контексте вопросов безопасности интерес представляет работа Н.В. Корнеева и А.Б. Дикого [5], посвященная разработке паттерна для обеспечения безопасности информационной инфраструктуры при миграции образов виртуальных машин. Авторы предлагают решение на основе микросервисной архитектуры, развёрнутой в контейнерах Docker, целью которого является защита от DoS-атак в процессе переноса данных. Данное исследование носит общий характер и не фокусируется на отечественной платформе виртуализации zVirt 4.5 и особенностях работы с форматом OVA.

Проведённый анализ источников свидетельствует об отсутствии экспериментальной работы, в ходе которой была бы произведена миграция виртуальных машин с Virtual Appliance (OVA) на отечественную платформу с учётом аспектов надёжности и безопасности.

Анализ предметной области

Миграция виртуальной машины представляет собой процесс перемещения работающей или остановленной виртуальной машины с одного хоста на другой. Данный процесс включает полное сохранение состояния машины, включая в себя содержимое оперативной памяти, состояние процессорных регистров, конфигурацию подключённых устройств и данные виртуальных дисков. Операция миграции виртуальной машины является критической для современных центров обработки данных, поскольку позволяет обеспечивать непрерывность работы приложений и балансировать нагрузку между физическими серверами.

Существует два типа миграции. Первый предполагает миграцию без остановки виртуальной машины – горячая миграция [6]. Процесс данной миграции в реальном времени переносит работающую ВМ с одного узла на другой. Все свойства ВМ, в том числе IP-адреса, метаданные, память, состояние сетей, операционных систем и приложений, остаются неизменными. Выбираемый для миграции целевой узел должен быть активен [7]. Второй тип — с остановкой ВМ: виртуальная машина недоступна на время миграции. Данный тип миграции называется холодной миграцией [6]. Этот процесс копирует дисковые образы, конфигурацию и метаданные на целевой узел без передачи оперативной памяти, поскольку она очищается при

выключении. Миграция с Virtual Appliance (OVA) на платформу zVirt 4.5 относится ко второму типу. Это можно объяснить тем, что ВМ полностью останавливается для создания экспортного образа, затем выполняется перенос и конвертация. На последнем шаге виртуальная машина импортируется и запускается на новой платформе.

Формат OVA (Open Virtualization Appliance) представляет собой каталоги в формате OVF – стандартном формате программ виртуальных устройств. Отличительная черта данного формата состоит в том, что все компоненты сохраняются в одном архиве. Для этого используется метод упаковки TAR. Это облегчает распространение данных виртуальных машин [9]. Платформа zVirt 4.5 использует собственные форматы виртуальных дисков (QCOW2, RAW), имея собственные требования к конфигурации виртуальных устройств. Эти особенности создают необходимость преобразования импортируемых образов, корректировки параметров виртуальных машин и проверки их работоспособности после переноса [10].

Надёжность миграции заключается в корректности виртуальной машины после переноса. Целостность виртуальных дисков является важным фактором при конвертации из исходного формата в целевой [8]. Ошибки при конвертации могут привести к невозможности загрузки операционной системы (далее – ОС). Формат Virtual Appliance (OVA) состоит из нескольких файлов, и повреждение или изменение их может привести к некорректной работе виртуальной машины, что обуславливает необходимость проверки целостности исходного образа. Для обеспечения надёжности выполняется тестовый запуск виртуальной машины, проверка работоспособности сервисов, корректности сетевых настроек.

В Российской Федерации ключевым документом, устанавливающим требования к средствам виртуализации, является Приказ ФСТЭК России № 187 от 27.10.2022 «Об утверждении требований по безопасности информации к средствам виртуализации» [11]. Требования приказа направлены на обеспечение конфиденциальности, целостности и доступности информации.

При соблюдении конфиденциальности данные мигрированной виртуальной машины не должны быть раскрыты. Злоумышленник может получить доступ к виртуальной машине, если на системе не настроены права доступа (NTFS/ACL) или они были сброшены в процессе миграции.

При обеспечении целостности данные и состояние ВМ не должны быть изменены, повреждены или подменены в процессе миграции. Повреждение файлов мигрирующей машины может произойти из-за аппаратных сбоев или ошибок в программных инструментах конвертации и передачи данных, приводя к изменению структуры OVA-образа.

Доступность определяется тем, что сервисы, работающие на виртуальной машине, должны оставаться доступными для пользователя после процесса миграции. Неудачная попытка миграции виртуальной машины с Virtual Appliance (OVA) в среду zVirt 4.5 приводит к изменению OVA-образа. Данный фактор может привести к неработоспособности виртуальной машины после процесса миграции.

Безопасность миграции заключается в защите данных переносимой виртуальной машины. Значимую роль в вопросе безопасности играют файлы с журналами событий, используемые для аудита и анализа событий.

Вопросы надёжности и безопасности миграции виртуальной машины с Virtual Appliance (OVA) в среду zVirt 4.5 включают проверку целостности данных, а также верификацию работоспособности сервисов, контроль корректности сетевых настроек, просмотр журналов с логами.

Проведение эксперимента

Для реализации процесса миграции виртуальных машин с Virtual Appliance (OVA) в среду zVirt 4.5 был выполнен эксперимент, включающий развертывание среды zVirt 4.5, настройку конфигурации процедуры миграции виртуальных машин из формата Virtual Appliance (OVA). Данный эксперимент направлен на тестирование холодной миграции с аспектами на вопросы надёжности и безопасности.

Рубрика 2. Методы и системы защиты информации, информационная безопасность

Были использованы виртуальные машины (далее – ВМ) с конфигурацией, представленной в таблице 1.

Таблица 1 – Конфигурация используемых виртуальных машин

Объект	ОС	RAM, ГБ	CPU, МБ	Размер диска, ГБ	IP-адрес	FQDN
Host 1	zVirt Node 4. 5	6	5	150	192.168.105.123/24	host1.vlab.local
NFS-хранилище	zVirt Node 4.5	4	4	150	192.168.105.162/24	nfs.vlab.local
CLI	РЕД 8.0.2	4	2	100	192.168.105.185/24	cli.vlab.local
Менеджер управления	-	4	4	61	192.168.105.13/24	engine.vlab.local
Мигрирующая виртуальная машина	Microsoft Windows 10	4	4	30	192.168.105.182/24	-

Для проведения эксперимента был развернут тестовый стенд на базе платформ ОС zVirt Node 4.5 и ОС РЕД 8.0.2. Архитектура стенда построена под задачу отработать миграцию виртуальной машины с Virtual Appliance (OVA) в среду zVirt 4.5. Выделены три основные машины. Первая Host 1 – машина с гипервизором, где работают виртуальные машины и развернут менеджер управления. Вторая NFS-хранилище – машина, на которой развернуто сетевое хранилище для хранения данных о виртуальных машинах. Третья машина выступает в роли клиента и обеспечивает доступ к веб-интерфейсу, так как первая и вторая машины имеют консольный режим (рис. 1). Миграция виртуальной машины win1 будет происходить с машины Admin-PC с платформы VMware Workstation Pro 25H2 [12].

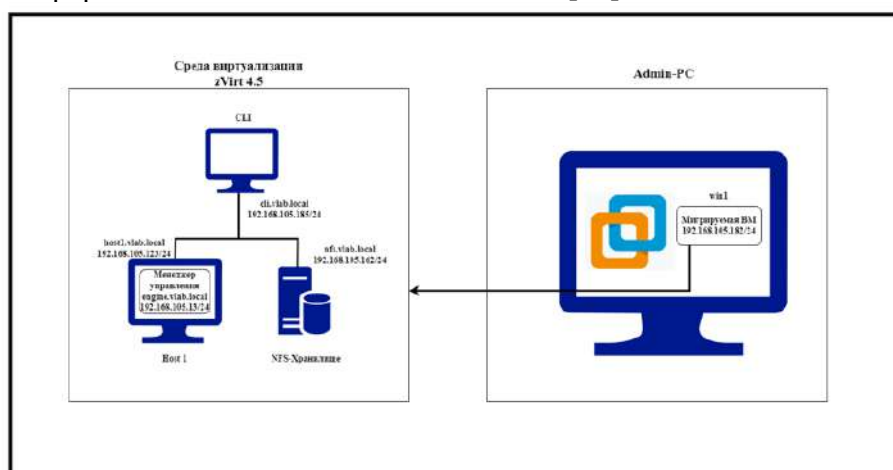


Рис. 1. Структура экспериментального стенда для миграции виртуальной машины в среду zVirt 4.5

Для начала эксперимента производится назначение IP-адресов и FQDN на устройствах согласно таблице 1 (рис.2 – рис.4).



Рис. 2. Назначение IP-адреса и FQDN на узле host1.vlab.local



Рис. 3. Назначение IP-адреса и FQDN на узле nfs.vlab.local

```

[root@cli ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:eb:78:c4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.105.123/24 brd 192.168.105.255 scope global dynamic noprefixroute
        valid_lft 86782sec preferred_lft 86782sec
    inet6 fe80::a80:27ff:feeb:78c4/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@cli ~]# cat /etc/hostname
cli.vlab.local
[root@cli ~]#

```

Рис. 4. Назначение IP-адреса и FQDN на клиентской машине cli.vlab.local

На каждой машине прописывается FQDN в файл /etc/hosts (рис. 5).

```

127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.105.123 host1.vlab.local
192.168.105.162 nfs.vlab.local
192.168.105.13 engine.vlab.local

```

```

GNU nano 2.9.8 /etc/hosts
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.105.123 host1.vlab.local
192.168.105.162 nfs.vlab.local
192.168.105.13 engine.vlab.local

```

Рис. 5. Заполнение файла /etc/hosts для сопоставления IP-адресов и FQDN узлов стенда

Для подготовки хранилища происходит создание каталога, в котором должно быть больше 55 ГиБ свободного места, а также установка прав доступа (рис. 6).

```

[root@nfs ~]# mkdir -p /storage/domain
[root@nfs ~]# chown vlsn:kun /storage/domain
[root@nfs ~]# chmod 0775 /storage/domain
[root@nfs ~]#

```

Рис. 6. Создание каталога NFS-хранилища и настройка прав доступа

Далее добавляется запись /storage/domain *(rw,anonuid=36,anongid=36) для NFS-сервера. Затем происходит запуск необходимых сервисов и создание правила межсетевого экрана.

На машине, выполняющей роль хоста, производится настройка репозиторий и развертывание менеджера управления. Затем с помощью команды hosted-engine --deploy начинается процесс установки менеджера управления. При развёртывании менеджера управления указываются его параметры согласно таблице 1.

Далее при корректной установке менеджера управления можно получить доступ к веб-интерфейсу по адресу <https://engine.vlab.local/ovirt-engine/> (рис.7).

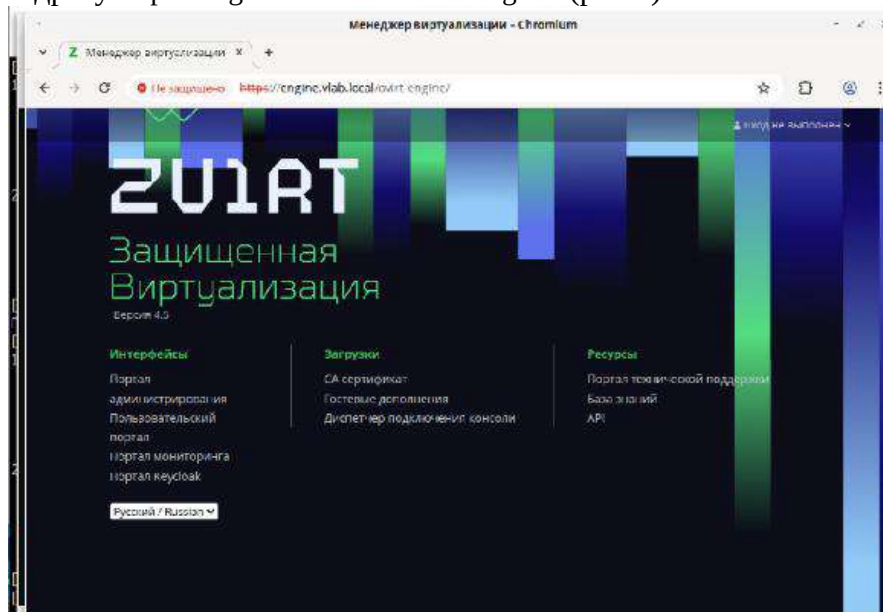


Рис. 7. Веб-интерфейс менеджера управления zVirt 4.5

Рубрика 2. Методы и системы защиты информации, информационная безопасность

После развёртывания менеджера управления происходит добавление хостов и хранилища.

Для импорта виртуальной машины из Virtual Appliance (OVA) в среду zVirt 4.5 дисковым форматом является VMDK. Перед тем, как импортировать виртуальную машину win1 в среду zVirt 4.5, делается экспорт из платформы VMware Workstation Pro 25H2.

Далее каталогу /data присваиваются права доступа 660 и владельцы: группа 36:36. В данном каталоге находится образ формата OVA (рис.8).

```
cd /data/  
ls  
cd /  
chown 36:36 /data/win1.ova  
chmod 660 /data/win1.ova
```

```
root@host1 /# cd /data/  
root@host1 data# ls  
images win1.ova  
root@host1 data# cd /  
root@host1 /# chown 36:36 /data/win1.ova  
root@host1 /# chmod 660 /data/win1.ova
```

Рис. 8. Настройка прав доступа к каталогу с OVA-файлом виртуальной машины

Затем через менеджер управления выполняется импорт машины в среду виртуализации zVirt 4.5. На первом шаге импорта происходит указание хоста и пути к OVA-файлу на NFS-хранилище (рис. 9).

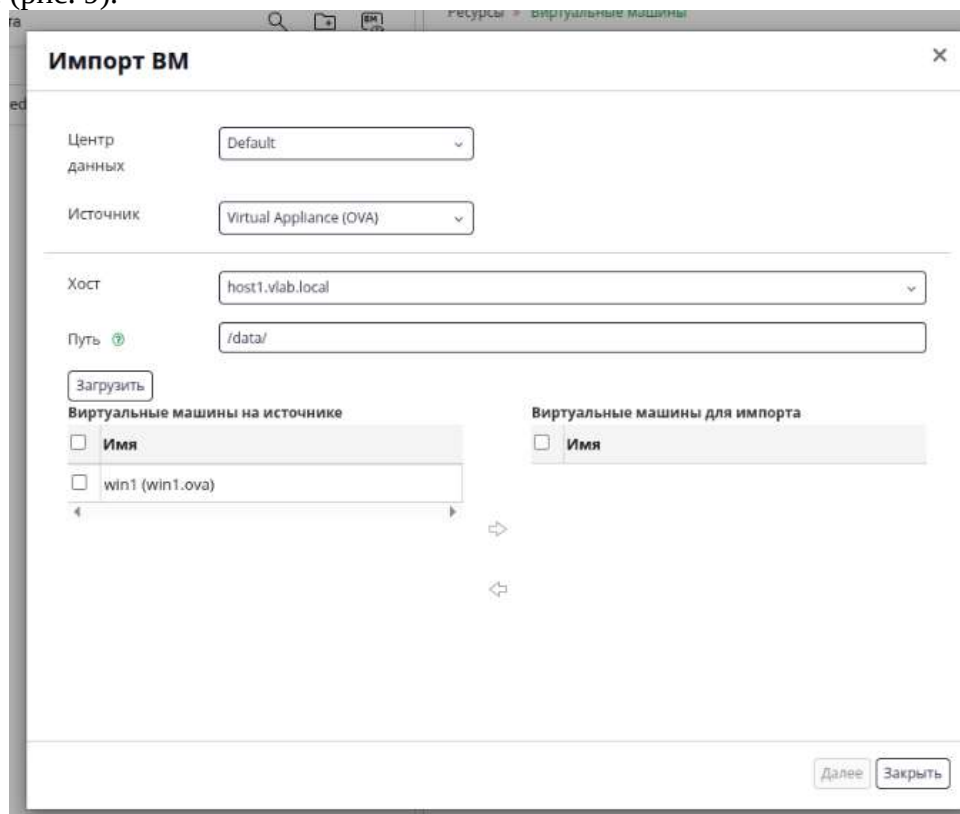


Рис. 9. Выбор хоста и пути к OVA-файлу при импорте виртуальной машины

На втором шаге задаются параметры импортируемой машины: целевой домен хранения hostedstorage, целевой кластер и профиль центрального процессора (далее – ЦП) по умолчанию, имя win1, а также выбирается импортируемая операционная система Windows 10. Остальные параметры были оставлены по умолчанию (рис. 10 – рис. 12).

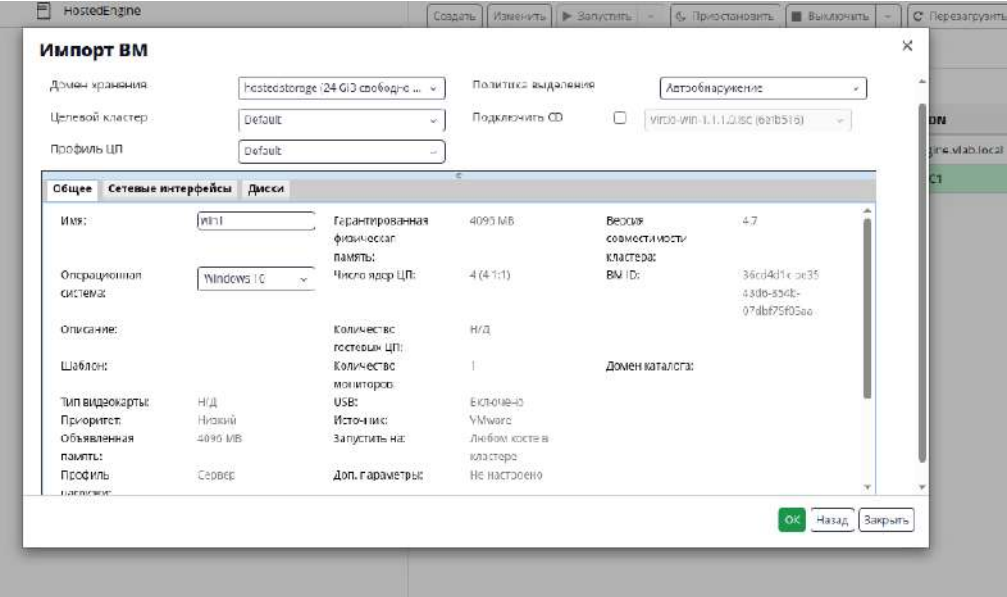


Рис. 10. Настройка целевого домена хранения при импорте виртуальной машины

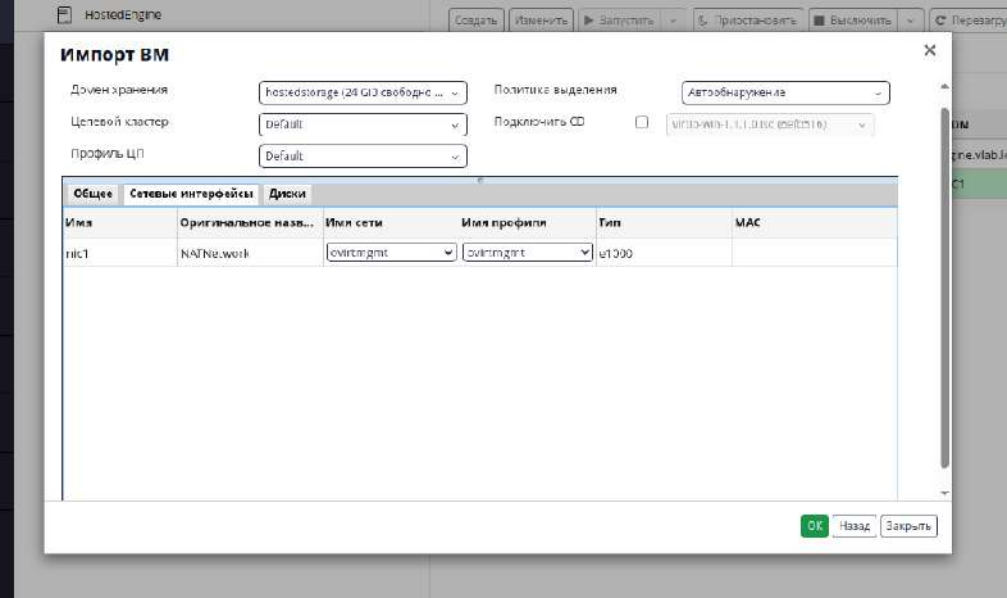


Рис. 11. Настройка параметров кластера и профиля процессора при импорте виртуальной машины

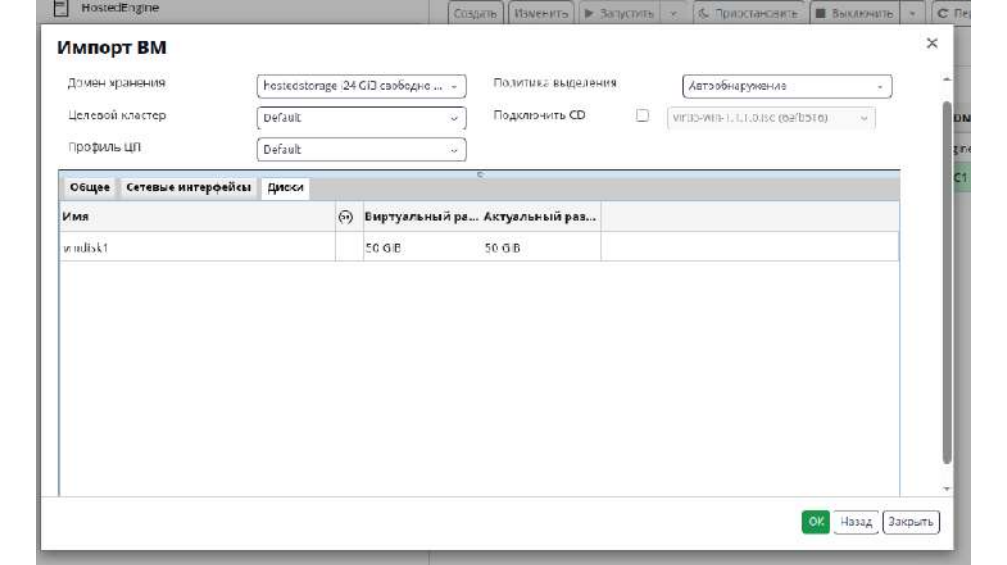


Рис. 12. Выбор операционной системы и имени импортируемой виртуальной машины

Рубрика 2. Методы и системы защиты информации, информационная безопасность

Импорт OVA-файла происходит напрямую в zVirt 4.5 через веб-интерфейс на хосте host1.vlab.local, с автоматической конвертацией дисков VMDK в QCOW2/RAW и настройкой интерфейсов VirtIO. Служба управления хостами zVirt 4.5 (VDSM) вызывает qemu-img convert для конвертации дисков из VMDK в QCOW2/RAW с VirtIO; диски импортируются в домен хранения без ручного ввода команд. Виртуальная машина win1 была сконвертирована в формат RAW (рис. 13).

```
[root@host1 34b4fdb2-f527-4f29-8d6b-b3f48f10f085]# qemu-img info /rhev/data-center/mnt/nfs:_storage_testzvirt/eb71cfa0-246c-4868-8fef-40b153fdb5d6/images/34b4fdb2-f527-4f29-8d6b-b3f48f10f085/c7b72181-f7c6-4f97-92c7-261b93a647b9
image: /rhev/data-center/mnt/nfs:_storage_testzvirt/eb71cfa0-246c-4868-8fef-40b153fdb5d6/images/34b4fdb2-f527-4f29-8d6b-b3f48f10f085/c7b72181-f7c6-4f97-92c7-261b93a647b9
file format: raw
virtual size: 50 GiB (53687091200 bytes)
disk size: 12.9 GiB
[root@host1 34b4fdb2-f527-4f29-8d6b-b3f48f10f085]#
```

Рис. 13. Результат импорта виртуальной машины в среду zVirt 4.5

В ходе эксперимента была успешно мигрирована ВМ с операционной системой Microsoft Windows 10. После запуска в среде отечественной платформы виртуализации zVirt 4.5 работоспособность операционной системы, сетевые подключения и базовые сервисы были полностью сохранены (рис. 14–15).

Ресурсы > Виртуальные машины > win1									
Искать Запустить В-Панель задач Выключить Перезагрузить Консоль Создать snapshot Импортировать									
Общие	Сетевые интерфейсы	Диски	Свойства	Приложения	Контейнеры	Устройства жест	Устройства VM	Группы снапшот	Метки снапшот
Гостевой агент	Разрешения	История	Резервные копии	События					
Имя:	win1		Облачная платформа:		4096 MB				
Описание:			Гарантированная физическая память:		4096 MB		ИСТОЧНИК		VirtualBox
Платформа:	64-битная x86_64		Совместимость:		не настроено		загружен		забыл пароль в консоли
Основа работы (платформа):	Linux		Число ядер:		4 (4 vCPU)		Хост: виртуальный		Host: VirtualBox не настроено
Операционная система:	Windows 10		Количество гостевых ЦП:		1 vCPU		Версия совместимости:		4.7
Тип BIOS:	Чипсет Q35 с BIOS		Тип ЦП:		amd64/hypervisor, amd64/t		VM ID:		360447c6-8d30-42d9-b54b-010000000000
Профилирование:	нет		Выходные документы:		нет		Класс:		Деловая категория
Настройка:	нет		Классификация:		нет		Аппаратный часовой пояс:		CMT Standard Time

Рис. 14. Параметры виртуальной машины после запуска в среде zVirt 4.5

[illegible]

Рис. 15. Проверка работоспособности виртуальной машины после миграции

Стоит отметить, что во вкладке «События» содержатся сообщения об успешном импорте машины win1 (рис.16).

[illegible]

Рис. 16. Сообщения о выполненном импорте виртуальной машины в журнале событий zVirt

Ключевой мерой обеспечения надёжности и безопасности стала верификация целостности OVA-образа. На исходной и целевой системах были вычислены хеш-суммы SHA-256 для OVA-образа. Хеш-суммы совпали между собой, что подтверждает целостность данных (рис. 17).

```
nano sha256sum.sh

#!/bin/bash

FILE="/data/win1.ova"
EXPECTED="16c77b7e5b858f1c1767a8b8817d0341a43281f165ce8caceedea78a6c84b626"

ACTUAL=$(sha256sum "$FILE" | awk '{print $1}')

if [ "$EXPECTED" = "$ACTUAL" ]; then
    echo "Файл цел"
else
    echo "Файл поврежден"
fi

echo "Ожидалось: $EXPECTED"
echo "Получено : $ACTUAL"

chmod +x sha256sum.sh
sh sha256sum.sh
```

```
[root@host1 ~]# chmod +x sha256sum.sh
[root@host1 ~]# sh sha256sum.sh
Файл цел
Ожидалось: 16c77b7e5b858f1c1767a8b8817d0341a43281f165ce8caceedea78a6c84b626
Получено : 16c77b7e5b858f1c1767a8b8817d0341a43281f165ce8caceedea78a6c84b626
[root@host1 ~]#
```

Рис. 17. Сравнение SHA-256 хеш-сумм OVA-образа на исходной и целевой системах

В рамках обеспечения безопасности были проанализированы журналы аудита, которые подробно описывают импорт ВМ из среды VMware, включая ошибки, что важно при расследовании инцидентов (рис. 18).

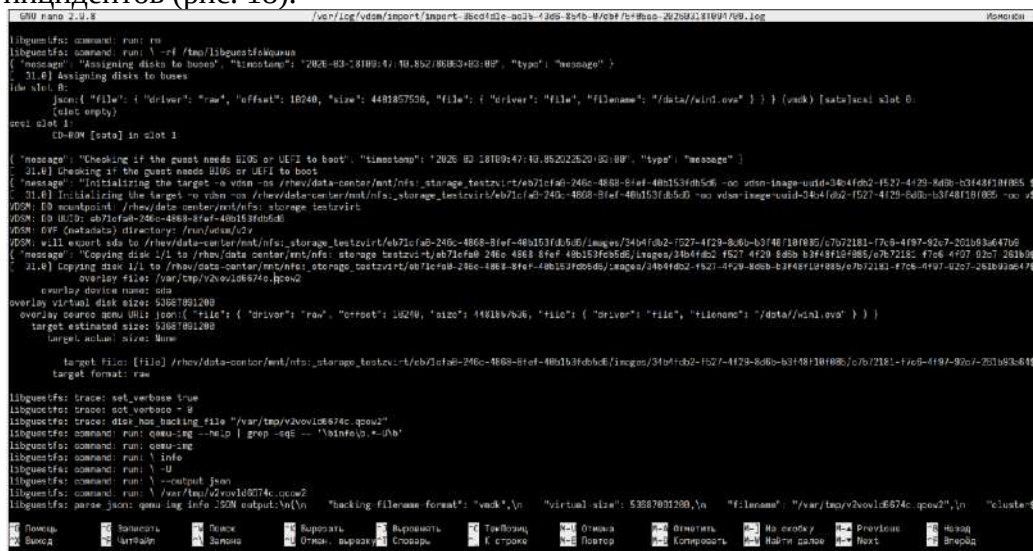


Рис. 18. Анализ лог-файла с событиями импорта виртуальной машины

Для минимизации человеческого фактора в веб-интерфейсе реализованы защитные механизмы. Они блокируют опасные операции, такие как запуск ВМ без диска (с выводом диагностики), а при удалении объектов запрашивают подтверждение и оставляют записи в логах аудита.

Проверка сохранения прав доступа NTFS/ACL в ОС Microsoft Windows 10 после миграции из Virtual Appliance (OVA) в среду zVirt 4.5 подтверждает безопасность процесса миграции (рис. 19). На виртуальной машине win1 до импорта выполнялась команда icacls C:\Users

Рубрика 2. Методы и системы защиты информации, информационная безопасность

/save C:\pre.acl /T и после icaccls C:\Users /save C:\post.acl /T. Затем происходит сравнение файлов pre.acl с post.acl с помощью команды fc C:\pre.acl C:\post.acl.

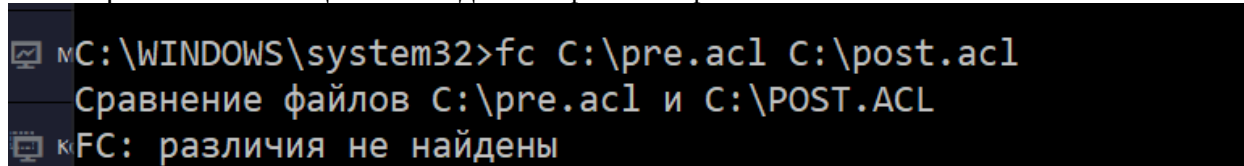


Рис. 19. Сравнение файлов pre.acl и post.acl для проверки сохранения прав доступа NTFS/ACL

Проведённый эксперимент позволяет верифицировать выполнение требований Приказа ФСТЭК России №187 от 27.10.2022 [11]. В таблице 2 соотнесены результаты эксперимента с соответствующими пунктами приказа по трём аспектам безопасности: целостность, конфиденциальность, доступность.

Таблица 2 – Требования приказа ФСТЭК России №187 от 27.10.2022

Аспект безопасности	Нормативное требование	Выполненная проверка	Результат проверки
Целостность	п. 10.1: контроль целостности объектов виртуализации. п. 10.3: обеспечение целостности сведений о событиях безопасности.	1. Выполнено сравнение SHA-256 хеш-сумм OVA-образа на исходной и целевой системах. 2. Проанализированы журналы событий, сформированные в процессе импорта виртуальной машины.	1. Хеш-суммы совпали, что подтверждает отсутствие изменений OVA-образа при переносе (рис. 17). 2. Журналы содержат сведения о выполненном импорте и позволяют отследить события миграции (рис. 18).
Конфиденциальность	п. 8: реализация функций управления доступом.	Выполнена проверка сохранения прав доступа NTFS/ACL внутри гостевой ОС Microsoft Windows 10. До миграции был создан файл pre.acl, после миграции — файл post.acl. Затем файлы были сравнены командой fc.	Списки контроля доступа NTFS/ACL совпали, что подтверждает сохранение исходных прав доступа после миграции виртуальной машины (рис. 19).
Доступность	п. 18.2: управление размещением и перемещением виртуальных машин с сохранением их конфигурации и настроек. п. 13.1: резервное копирование образов виртуальных машин и конфигурации виртуального оборудования.	1. Выполнена холодная миграция виртуальной машины из OVA-формата в среду zVirt 4.5. 2. Проверены запуск виртуальной машины, сетевые параметры и базовая работоспособность ОС после импорта. 3. Перед миграцией был создан OVA-образ, используемый как резервная копия исходной виртуальной машины.	1. Виртуальная машина успешно импортирована и запущена в среде zVirt 4.5 (рис. 13–14). 2. Работоспособность ОС и сетевых подключений после миграции подтверждена (рис. 15–16). 3. Использование OVA-образа обеспечило возможность восстановления или повторного импорта виртуальной машины.

Среда виртуализации zVirt 4.5 обеспечивает холодную миграцию с сохранением безопасности: целостность данных, конфиденциальность прав доступа, доступность виртуальной машины. Требования ФСТЭК №187 верифицированы экспериментально.

Заключение

Проведенный эксперимент показывает, что платформа виртуализации zVirt 4.5 реализует комплексный многоуровневый подход к информационной безопасности, сочетающий различные меры защиты. Экспериментальным путем подтверждена работоспособность миграции, а также рассмотрены вопросы безопасности и надёжности: успешное сравнение хеш-сумм, анализ журналов событий, сравнение прав доступа на мигрированной машине. Однако холодная миграция имеет существенные недостатки в реализации надёжности и безопасности: полная остановка ВМ, отсутствие продолжения работы приложений.

Библиографический список

1. Importing a Virtual Machine OVA into Proxmox [Электронный ресурс] // i12bretro. – URL: <https://i12bretro.github.io/tutorials/0387.html> (дата обращения: 10.01.2025).
2. Конвертация OVA/OVF для миграции с VMware на Hyper-V [Электронный ресурс] // Vinchin. – URL: <https://www.vinchin.com/ru/vm-migration/hyper-v-ova-ovf.html> (дата обращения: 10.01.2025).
3. Попок, Л. Е. Методика миграции виртуальных нагрузок с платформы виртуализации VMware vSphere на платформу виртуализации Microsoft Hyper-V / Л. Е. Попок, А. Е. Богомолов // КубГАУ. – 2019. – № 153. – С. 1–15.
4. Цыганкова, А. А. Применение технологии виртуализации в образовательном процессе университета: сравнительный анализ отечественных платформ виртуализации / А. А. Цыганкова, К. П. Климченко // Наукосфера. – 2023. – № 5. – С. 1–7.
5. Корнеев, Н. В. Паттерн для обеспечения безопасности информационной инфраструктуры при миграции образов виртуальных машин / Н. В. Корнеев, А. Б. Дикий // Cyberleninka. – 2025. – С. 12.
6. Миграция виртуальных машин [Электронный ресурс] // ISPSystem. – URL: <https://www.ispsystem.ru/docs/vmmanager-admin/virtual-nye-mashiny/migratsiya-virtual-nyh-mashin> (дата обращения: 13.12.2025).
7. Как конвертировать форматы образов виртуальных машин [Электронный ресурс] // Arenda Server. – URL: <https://arenda-server.cloud/blog/kak-konvertirovat-formaty-obrazov-virtualnyh-mashin/> (дата обращения: 20.12.2025).
8. OVA — Open Virtual Appliance [Электронный ресурс] // Online-Convert. – URL: <https://www.online-convert.com/ru/file-format/ova> (дата обращения: 02.12.2025).
9. zVirt 4.5 [Электронный ресурс] // Orion Soft Wiki. – URL: <https://wiki.orionsoft.ru/zvirt/> (дата обращения: 02.12.2025).
10. Как мигрировать ВМ с VMware на zVirt? [Электронный ресурс] // Vinchin. – URL: <https://www.vinchin.com/ru/vm-migration/migratsiya-vm-s-vmware-na-zvirt.html> (дата обращения: 02.12.2025).
11. Приказ ФСТЭК России от 27 октября 2022 г. № 187 «Об утверждении требований по безопасности информации к средствам виртуализации» [Электронный ресурс] // Официальный интернет-портал ФСТЭК России. – 2022.
12. Fusion and Workstation [Электронный ресурс] // VMware. – URL: <https://www.vmware.com/products/desktop-hypervisor/workstation-and-fusion> (дата обращения: 20.12.2025).

References

1. i12bretro. (n.d.). *Importing a virtual machine OVA into Proxmox*. Retrieved January 10, 2025, from <https://i12bretro.github.io/tutorials/0387.html>
2. Vinchin. (n.d.). *Converting OVA/OVF for migration from VMware to Hyper-V*. Retrieved January 10, 2025, from <https://www.vinchin.com/ru/vm-migration/hyper-v-ova-ovf.html>
3. Popok, L. E., & Bogomolov, A. E. (2019). Methodology for migrating virtual workloads from the VMware vSphere virtualization platform to the Microsoft Hyper-V virtualization platform. *KubSAU*, 153, 1–15.
4. Tsygankova, A. A., & Klimchenko, K. P. (2023). Application of virtualization technology in the educational process of a university: A comparative analysis of domestic virtualization platforms. *Naukasfera*, 5, 1–7.
5. Korneev, N. V., & Dikiy, A. B. (2025). Pattern for ensuring the security of information infrastructure during the migration of virtual machine images. *Cyberleninka*, 12.
6. ISPSystem. (n.d.). *Migration of virtual machines*. Retrieved December 13, 2025, from <https://www.ispsystem.ru/docs/vmmanager-admin/virtual-nye-mashiny/migratsiya-virtual-nyh-mashin>
7. Arenda Server. (n.d.). *How to convert virtual machine image formats*. Retrieved December 20, 2025, from <https://arenda-server.cloud/blog/kak-konvertirovat-formaty-obrazov-virtual-nyh-mashin/>

Рубрика 2. Методы и системы защиты информации, информационная безопасность

8. Online-Convert. (n.d.). *OVA — Open Virtual Appliance*. Retrieved December 2, 2025, from <https://www.online-convert.com/ru/file-format/ova>
9. Orion Soft Wiki. (n.d.). *zVirt 4.5*. Retrieved December 2, 2025, from <https://wiki.orion-soft.ru/zvirt/>
10. Vinchin. (n.d.). *How to migrate VM from VMware to zVirt?* Retrieved December 2, 2025, from <https://www.vinchin.com/ru/vm-migration/migratsiya-vm-s-vmware-na-zvirt.html>
11. Federal Service for Technical and Export Control of Russia. (2022). *Order No. 187 of October 27, 2022: Information security requirements for virtualization tools*.
12. VMware. (n.d.). *Fusion and Workstation*. Retrieved December 20, 2025, from <https://www.vmware.com/products/desktop-hypervisor/workstation-and-fusion>

Информация об авторе

Андрианова Дарья Сергеевна – студент, РГУ нефти и газа (НИУ) имени И.М. Губкина, г. Москва, e-mail: andrianova.darya2002@gmail.com

MIGRATION OF VIRTUAL MACHINES FROM VIRTUAL APPLIANCE (OVA) TO ZVIRT. RELIABILITY AND SAFETY ISSUES

Andrianova D. S.¹

¹*National University of Oil and Gas «Gubkin University»*

Abstract. The article examines the migration of virtual machines from the Virtual Appliance (OVA) format, used in VMware and VirtualBox hypervisors, to the domestic virtualization platform zVirt version 4.5. The relevance of the study is determined by the need to replace foreign virtualization platforms and to ensure reliability and security during the transfer of virtual infrastructure. The purpose of the work is to experimentally verify the possibility of cold migration of a virtual machine to the zVirt 4.5 environment while preserving its operability and basic security parameters.

During the study, an experimental testbed was designed and deployed. It included a virtualization host, NFS storage, and a management engine. The testbed was used to migrate a virtual machine running Microsoft Windows 10 from the OVA format to the zVirt environment. Special attention was paid to converting the virtual disk from the VMDK format to the target format, checking the correctness of the import procedure, preserving network parameters, and verifying the operation of the virtual machine after migration.

The results of the experiment confirmed the possibility of successful cold migration of a virtual machine to the zVirt 4.5 platform. To assess reliability and security, SHA-256 hash sums of the source and transferred OVA image were compared, event logs were analyzed, and NTFS/ACL access rights were checked. The obtained results show that, with proper infrastructure preparation, migration can be performed while maintaining data integrity, virtual machine operability, and control over the transfer process.

Keywords: *zVirt, Virtual Appliance, OVA, hash sum, reliability, security, migration.*

Information about the author

Andrianova Darya Sergeevna — student, Gubkin Russian State University of Oil and Gas, Moscow, e-mail: andrianova.darya2002@gmail.com