Утвержден

РДЦП.10001-02-УД

ПРОГРАММНЫЙ КОМПЛЕКС «СРЕДСТВА ВИРТУАЛИЗАЦИИ «БРЕСТ»

Описание применения

РДЦП.10001-02 31 01

Листов 23

2022

Литера $О_1$

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

АННОТАЦИЯ

Настоящий документ является описанием применения программного изделия «Программный комплекс «Средства виртуализации «Брест» (ПК СВ «Брест») РДЦП.10001-02 (далее по тексту — ПК СВ).

В документе приведены назначение ПК СВ, условия применения, описание задачи, а также приведено описание входных и выходных данных ПК СВ.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1. Назначение

ПК СВ предназначен для создания виртуальной среды, обеспечивающей функционирование виртуальных машин и управление ими в операционной системе специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (далее по тексту — ОС СН).

1.2. Область применения

Информационные (автоматизированные) системы, обрабатывающие общедоступную информацию и информацию ограниченного доступа.

1.3. Возможности

Изделие функционирует под управлением ОС СН и совместно с ней предоставляет следующие возможности:

- создание виртуальных машин (ВМ), их образов и шаблонов с помощью графического и консольного интерфейсов с поддержкой 32 и 64-битных гостевых операционных систем (ОС);
- создание ВМ из настраиваемых шаблонов;
- управление конфигурацией ВМ с помощью графического и консольного интерфейсов;
- обеспечение возможности централизованного управления кластерами, серверной частью изделия на всех узлах кластера высокой доступности, хранилищами и виртуальными коммутаторами;
- обеспечение мониторинга работоспособности и использования ресурсов виртуальными машинами и серверной частью изделия и генерации отчетов, в т.ч. за выбранный период с возможностью выдачи оповещения на интерфейс управления при превышении пороговых значений метрик использования ресурсов;
- поддержку виртуальных коммутаторов с технологией VLAN (Virtual Local Area Network);
- изменение без завершения функционирования ВМ количества выделенных им процессоров и размера оперативной памяти;
- подключение к ВМ устройств из состава аппаратных средств, на которых функционирует серверная часть изделия, включая устройства USB 3.0;
- подключение к ВМ по протоколу SPICE USB-устройств из состава аппаратных средств, на которых функционирует клиентская часть изделия;
- добавление виртуальных дисков в гостевую операционную систему и увеличение их размеров без остановки ВМ;

- поддержку открытого стандарта для хранения и распространения виртуальных машин Open Virtualization Format (OVF);
- обеспечение возможности клонирования ВМ;
- управление приоритетом дисковых операций ввода-вывода для ВМ;
- выполнение миграции работающих ВМ между узлами кластера без прерывания работы в автоматическом и ручном режимах;
- обеспечение возможности миграции функционирующих ВМ между узлами без прерывания сетевых соединений ВМ;
- обеспечение возможности ограничения сетевого и дискового ввода-вывода виртуальных машин на основе их групповых или индивидуальных настроек;
- автоматическое распределение сервером виртуализации ресурсов между работающими ВМ;
- обеспечение возможности централизованного хранения конфигурационной информации о ВМ и среде виртуализации;
- обеспечение возможности создания копий трафика виртуальных машин внутри виртуального сетевого коммутатора на его сетевой порт;
- обеспечение возможности создания резервных копий виртуальных машин, а также последующего восстановления.

При этом средствами ОС СН обеспечиваются следующие возможности по созданию и защите среды виртуализации:

- эмуляция аппаратного обеспечения с использованием аппаратных возможностей архитектуры x86-64 по виртуализации процессоров на основе модуля KVM (Kernel-based Virtual Machine) из состава ОС СН;
- поддержка в ВМ до 240 виртуальных процессоров (физических ядер);
- поддержка в ВМ до 4000 ГБ оперативной памяти;
- поддержка IPMI 2.0;
- поддержка расширения количества управляемых ВМ до 10 000 (при наличии соответсвующей инфраструктуры серверов);
- возможность группового создания 500 и более ВМ из шаблонов;
- идентификация и аутентификация субъектов доступа (пользователей и администраторов) до предоставления доступа к функциям виртуализации и управления изделия, в том числе в режиме взаимодействия со средствами создания единого пространства пользователей (FreeIPA) из состава ОС СН;
- функционирование в условиях мандатного и дискреционного управления доступом ОС СН при межпроцессном и сетевом взаимодействии, включая взаимодействие между ВМ по протоколам стека IPv4 в условиях мандатного управления доступом и

доступ субъектов к файлам-образам и экземплярам функционирующих ВМ;

- запуск ВМ в виде отдельного процесса ОС СН, функционирующего от имени учетной записи субъекта доступа (пользователя) с унаследованием его мандатных атрибутов;

- обеспечение создания тонких (терминальных) клиентов с использованием технологии VDI (Virtual Desktop Infrastructure) с предоставлением удаленного доступа к ВМ по протоколам VNC и SPICE, в т.ч. в условиях установленных в ОС СН правил дискреционного и мандатного управления доступом;

- поддержка серверной частью изделия следующих механизмов оптимизации оперативной памяти: дедупликация страниц, динамическое распределение, выгрузка в файл подкачки;

- создание динамически расширяющегося виртуального дискового пространства ВМ с обеспечением возможности выделения соответствующих аппаратных средств (физических дисков, блоков физических дисков) по мере заполнения виртуального дискового пространства ВМ;

- обеспечение возможности создания кластеров высокой доступности, обеспечивающих отказоустойчивое функционирование ВМ посредством репликации файлов ВМ между системами хранения и миграции ВМ между узлами кластера;

- обеспечение возможности ручной балансировки нагрузки на вычислительные ресурсы аппаратных средств за счет перераспределения ВМ между узлами кластера;

- обеспечение маршрутизации сетевых пакетов ВМ;

- обеспечение возможности защиты файлов-образов ВМ от модификации в процессе функционирования ВМ;

- обеспечение возможности регистрации событий с использованием средств централизованного протоколирования из состава ОС СН;

- обеспечение возможности контроля сетевого трафика, передаваемого между ВМ с целью обнаружения (предупреждения) компьютерных атак;

- обеспечение возможности централизованного обновления изделия с использованием штатных средств ОС СН.

Защита информации в ПК СВ обеспечивается средствами защиты информации ОС СН.

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. Требования к программным средствам

ПК СВ функционирует только под управлением ОС СН не ниже 1.7.1 на максимальном уровне защищенности («Смоленск»). При этом допускается развертывание ПК СВ в сервисном режиме на физических серверах под управлением ОС СН, функционирующей на базовом уровне защищенности («Орел»).

2.2. Требования к техническим средствам

2.2.1. Обзор архитектуры

Основными программными компонентами облака ПК СВ являются (см. рис. 1):

- машина предварительной обработки данных (фронтальная машина) — сервис, обеспечивающий управление Узлами виртуализации. Также предоставляет веб-интерфейс администратора облака ПК СВ;
- узел виртуализации — сервис, предоставляющий необходимые вычислительные ресурсы для виртуальных машин;
- облачное хранилище данных — система, предназначенная для хранения образов дисков виртуальных машин. Может быть построена на базе следующих технологий хранения:
    - файловой технологии хранения (с использованием локальной файловой системы или кластерной файловой системы, например ocfs2),
    - блочной технологии хранения с использованием LVM,
    - объектной технологии хранения Ceph;
- контроллер домена — сервис, обеспечивающий аутентификацию и авторизацию пользователей (не используется в сервисном режиме работы ПК СВ).

Примечание. Если на объекте эксплуатации уже имеется настроенный домен FreeIPA, то разворачивать дополнительный контроллер домена нет необходимости. Все серверы вводятся в существующий домен.

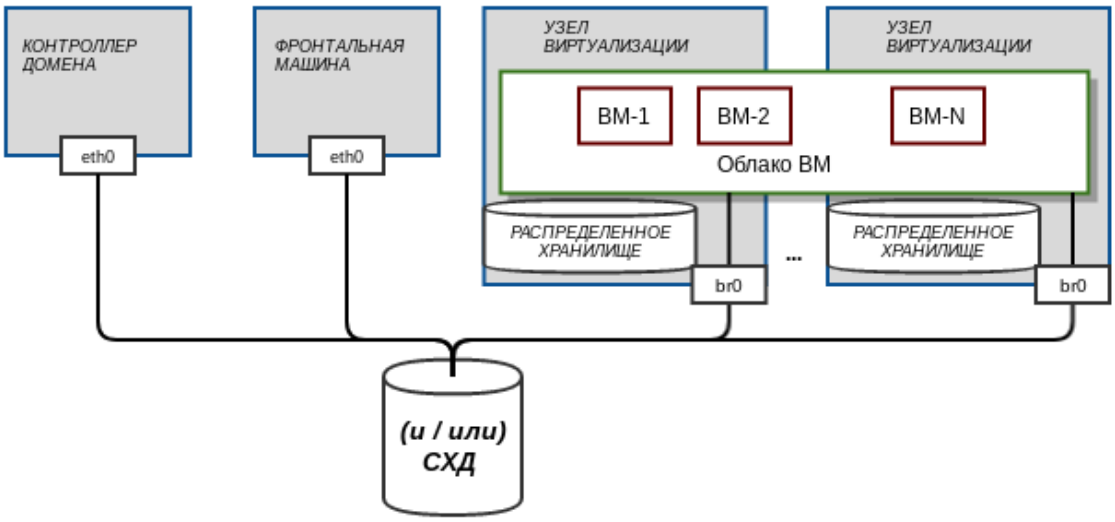

Рис. 1

Облако ПК СВ может быть развернуто как на группе физических серверов, так и на виртуальных машинах в пределах одного сервера или рабочей станции для стендирования. Для объединения физических серверов, обеспечения выполнения операций управления и поддержки облачных сетей для виртуальных машин используется физическая сеть. Для организации доступа к ВМ используется облачная (виртуальная) сеть. На рис. 1 отображен сетевой режим Bridged (сетевой мост) — ВМ доступны ресурсы физической локальной сети.

ВНИМАНИЕ! Программные компоненты облака ПК СВ должны функционировать на оборудовании, отвечающему требованиям к аппаратному обеспечению под управлением ОС СН.

В 2.2.1.1–2.2.1.2 приведены основные требования к техническим средствам, на которых планируется развернуть облако ПК СВ.

Примечание. Если для установки сервисов ПК СВ планируется использовать оптические установочные носители, то серверы должны быть оборудованы устройством для чтения и записи CD и DVD.

2.2.1.1. Требования фронтальной машины

Минимальные рекомендуемые характеристики сервера для развертывания сервиса фронтальной машины приведены в таблице 1.

Таблица 1

Ресурсы	Минимальная рекомендуемая конфигурация
Память	2 ГБ
ЦП	1 ЦП (2-ядерный)
Размер диска	100 ГБ
Сеть	2 NICS

Максимальное количество серверов (узлов виртуализации), которым можно управлять с помощью одного экземпляра фронтальной машины, зависит от производительности и масштабируемости инфраструктуры облака и главным образом от системы хранения данных. Не рекомендуется использовать один экземпляр фронтальной машины для управления более чем 500 серверами.

Фронтальная машина должна иметь сетевое соединение со всеми узлами виртуализации и, по возможности, доступ к хранилищам данных (как локальным, так и сетевым). Для обеспечения надежности облачной инфраструктуры рекомендуется использовать как минимум две сети (соответственно, требуется два сетевых интерфейса):

- сервисная сеть — используется сервисами фронтальной машины для обеспечения доступа к узлам виртуализации с целью управления и мониторинга гипервизоров и перемещения файлов образов;
- сеть экземпляров — обеспечивает возможность сетевого подключения к виртуальным машинам через различные узлы виртуализации.

Кроме того, может потребоваться третий сетевой интерфейс для обеспечения доступа к сети хранения данных.

Для базовой установки сервиса фронтальной машины требуется не более 150 МБ.

2.2.1.2. Требования узла виртуализации

Минимальные рекомендуемые характеристики сервера для развертывания сервиса узла виртуализации:

1) процессорная архитектура x86-64 с аппаратной поддержкой виртуализации (Intel VT, AMD-V);

2) центральный процессор (ЦП) — без последующих дополнительных нагрузок каждый модуль ЦП, закрепленный за одной ВМ, должен соответствовать физическому ядру ЦП в случае, если необходимо минимизировать конкуренцию ВМ за процессорные ядра. Например, при нагрузке в 40 виртуальных машин с двумя ЦП каждая для облака потребуются 80 физических ЦП. При этом 80 физических ЦП могут распределяться по различным узлам: 10 серверов с восемью ядрами каждый или пять серверов с 16 ядрами каждый. При необходимости последующих дополнительных нагрузок архитектуру ЦП можно планировать заранее с помощью элементов CPU и VCPU: CPU определяет физические ЦП, закрепленные за виртуальными машинами, а VCPU — виртуальные ЦП, передаваемые гостевой операционной системой;

3) оперативная память — по умолчанию в облаке ПК СВ отсутствует избыточно выделяемая память. Как правило, рекомендуется всегда предусматривать резерв 10 % по ресурсам, потребляемым гипервизором. Например, для нагрузки в 45 виртуальных машин с 2 ГБ оперативной памяти каждая необходимо 90 ГБ физической памяти.

Важным параметром является количество узлов, поскольку в связи с применением гипервизоров на каждый из них приходится 10 % затрат ресурсов. Например, 10 гипервизоров с 10 ГБ оперативной памяти каждый предоставят по 9 ГБ памяти, поэтому они смогут выдержать планируемую нагрузку;

4) объем свободного дискового пространства — не менее 30 Гб;

В каждом узле виртуализации в зависимости от конфигурации хранилища и сети должно быть установлено до четырех сетевых интерфейсов: для сети экземпляров (приватной и/или публичной), сервисной сети и сети хранения данных.

2.3. Порядок эксплуатации

Установка, настройка и эксплуатация ПК СВ осуществляется в соответствии с эксплуатационной документацией согласно РДЦП.10001-02 20 01 «Программный комплекс «Средства виртуализации «Брест». Ведомость эксплуатационных документов».

Дополнительная информация о порядке эксплуатации, а также варианты реализации отдельных решений приведены на официальном сайте `wiki.astralinux.ru`.

2.4. Порядок обновления

Для ПК СВ предусмотрен выпуск очередных (плановых) обновлений (новых версий) и выпуск внеочередных (оперативных) обновлений.

2.4.1. Очередное (плановое) обновление

Очередное (плановое) обновление ПК СВ представляет собой новую версию ПК СВ и решает следующий комплекс задач:

- реализация новых функциональных возможностей ПК СВ;
- устранение уязвимостей;
- повышение удобства использования и управления средствами виртуализации.

Лицензиаты (потребители) оповещаются о возможности и порядке получения очередного обновления ПК СВ как с использованием контактной информации, указанной в заключенных ранее лицензионных договорах (дополнениях к лицензионным договорам), так и путем размещения соответствующей информации на сайте разработчика `astralinux.ru`.

Получение очередного обновления ПК СВ осуществляется установленным порядком при заключении соответствующего лицензионного договора (дополнения к имеющемуся лицензионному договору).

Контроль целостности потребителями очередного обновления ПК СВ (входной контроль) осуществляется посредством подсчета контрольных сумм компакт-дисков. Значения контрольных сумм и порядок подсчета определены в документе РДЦП.10001-02 30 01 «Программный комплекс «Средства виртуализации «Брест». Формуляр».

Дополнительный контроль целостности файлов, входящих в состав очередного обновления ПК СВ, осуществляется:

- регламентно — средствами контроля целостности путем подсчета и сравнения контрольных сумм файлов ПК СВ с эталонными значениями, указанными в файле `gostsums.txt`, размещенном на установочном диске ПК СВ, в соответствии с описанием, приведенном в документе РУСБ.10015-01 97 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1»;
- автоматически — средствами ограничения программной среды в соответствии с описанием, приведенным в документе РУСБ.10015-01 97 01-1.

2.4.2. Внеочередное (оперативное) обновление

При получении сведений о наличии в компоненте ПК СВ уязвимости разработчик ПК СВ выпускает внеочередное обновление ПК СВ.

Внеочередное обновление ПК СВ может быть доступно в виде:

1) отдельных инструкций, содержащих сведения об обязательных к проведению при эксплуатации ПК СВ организационно-технических мероприятиях;
2) отдельных файлов программ, инструкций по их установке и настройке, а также информации, содержащей сведения о контрольных суммах всех файлов внеочередного обновления ПК СВ;
3) пакетов программ, инструкций по их установке и настройке, а также информации, содержащей сведения о контрольных суммах всех файлов внеочередного обновления ПК СВ;
4) методических указаний по настройке и особенностям эксплуатации ПК СВ с установленным внеочередным обновлением ПК СВ.

Лицензиаты (потребители) оповещаются о возможности и порядке получения внеочередного обновления ПК СВ как с использованием контактной информации, указанной в заключенных ранее лицензионных договорах (дополнениях к лицензионным договорам), так и путем размещения соответствующей информации на сайте разработчика `astralinux.ru`.

Контроль целостности внеочередных обновлений ПК СВ осуществляется посредством подсчета контрольных сумм с использованием программ подсчета контрольных сумм `gostsum` (для файлов) и `gostsum_from_deb` (для deb-пакетов) из состава ОС СН в соответствии с документом РУСБ.10015-01 97 01-1.

Дополнительный контроль целостности файлов, входящих в состав внеочередного обновления ПК СВ, осуществляется:

- регламентно — средствами контроля целостности путем подсчета и сравнения

контрольных сумм файлов ПК СВ с эталонными значениями, указанными в файле `gostsums.txt`, входящем в состав внеочередного обновления ПК СВ, в соответствии с описанием, приведенном в документе РУСБ.10015-01 97 01-1;

- автоматически — средствами ограничения программной среды в соответствии с описанием, приведенным в документе РУСБ.10015-01 97 01-1.

Источником внеочередного обновления ПК СВ для информационных (автоматизированных) систем, находящихся в компетенции ФСТЭК России, является соответствующий раздел на официальном сайте разработчика ПК СВ (`astralinux.ru/update`).

2.4.3. Контроль целостности обновлений

Для обеспечения контроля целостности объектов ПК СВ в состав дистрибутива входит файл `gostsums.txt` со списком контрольных сумм по ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит для всех файлов, входящих в пакеты программ дистрибутива. Используя утилиту `integrity-check` из состава ПК СВ можно провести подсчет контрольных сумм файлов системы и проверку соответствия подсчитанных контрольных сумм эталонным контрольным суммам.

Для проведения контроля целостности необходимо:

1) смонтировать установочный диск ПК СВ и перейти в каталог монтирования, например:

```
mount /dev/cdrom /mnt
cd /mnt
```

2) выполнить команду:

```
sh ./integrity-check ./gostsums.txt
```

3. ОСОБЕННОСТИ ЭКСПЛУАТАЦИИ ЗАЩИЩЕННОЙ СРЕДЫ ВИРТУАЛИЗАЦИИ

Функционирование защищенной среды виртуализации обеспечивается только в дискреционном режиме работы ПК СВ.

При проектировании защищенной среды виртуализации, предназначенной для применения в автоматизированных системах в защищенном исполнении, обрабатывающих информацию, ограниченного доступа, в том числе, содержащую сведения, составляющие государственную тайну, рекомендуется учитывать условия и ограничения, представленные далее.

Решение о применении и порядке применения указанных ограничений в качестве мер защиты информации должно приниматься в ходе проектирования системы защиты информации исходя из класса защищенности автоматизированной системы и угроз безопасности информации, включенных в модель угроз безопасности автоматизированной системы, а также с учетом ее структурно-функциональных характеристик.

Правила и процедуры по реализации требований о защите информации и мер защиты информации в конкретной автоматизированной системе определяются в эксплуатационной документации и организационно-распорядительных документах по защите информации.

3.1. Общие условия

3.1.1. Управление доступом внутри ОС виртуальной машины реализуется встроенными средствами защиты информации из состава ОС или сертифицированными наложенными средствами защиты информации.

3.1.2. Управление потоками информации между информационными системами, сегментами информационных систем, компонентами, функционирующими в виртуальной инфраструктуре и по периметру виртуальной инфраструктуры, осуществляется с помощью сертифицированных межсетевых экранов, не входящих в состав изделия.

3.1.3. Управление защищенной средой виртуализации реализуется с использованием выделенной сети управления.

3.1.4. Подключение внешних USB-устройств (перенаправление физических устройств узла виртуализации в ОС виртуальной машины) регламентируется дополнительными организационно-техническими мерами, состав которых подлежит согласованию с подразделением, ответственным за защиту информации.

3.1.5. При миграции ВМ не обеспечивается сохранение подключений USB и PCI-устройств к ВМ.

3.1.6. Не допускается использование сетевого устройства virtio для виртуальной машины, отличных от ОС СН.

3.2. Дополнительные условия, применяемые при реализации политики мандатного управления доступом

3.2.1. Управление потоками информации, в том числе при взаимодействии между ВМ, осуществляется с учетом классификационных меток, установленных по правилам и в формате в соответствии с национальным стандартом ГОСТ Р 58256-2018 «Защита информации. Управление потоками информации в информационной системе. Формат классификационных меток».

3.2.2. В случае, если ОС виртуальной машины не реализует мандатное управление доступом самостоятельно и/или не поддерживают классификационные метки по ГОСТ Р 58256-2018, запуск ВМ обеспечивается с уровнем, соответствующим уровню доступа работы пользователя. В таком случае, мандатное управление доступом на основе классификационной метки процесса ВМ и соответствующей маркировки сетевых пакетов обеспечивается ОС СН узла виртуализации. В целях исключения установки вредоносного программного обеспечения и хранения защищаемых данных в виртуальном диске используется режим запуска ВМ «Только для чтения».

Режим запуска ВМ «Только для чтения» регламентируется дополнительными организационно-техническими мерами, состав которых согласуется с подразделением, ответственным за защиту информации.

3.2.3. В случае, если ОС виртуальной машины реализует мандатное управление доступом и поддерживают классификационные метки по ГОСТ Р 58256-2018 запуск ВМ выполняется с учетом организационно-технических мер и в соответствии с политикой разграничения доступа на объекте информатизации одним из разрешенных способов:

1) в режиме «Только для чтения» с классификационной меткой, равной нулю (0), в целях исключения влияния средств мандатного управления доступом ОС СН узла виртуализации на маркировку сетевых пакетов, выполненную средствами защиты информации ОС виртуальной машины;

2) в режиме «Только для чтения» при соответствии уровня конфиденциальности сессии пользователя, инициирующего запуск ВМ, и уровня конфиденциальности сеанса в ОС виртуальной машины, так, чтобы средства ОС СН узла виртуализации заменяли значения классификационных меток, ранее установленные ОС виртуальной машины, на то же самое значение;

3) без включения режима «Только для чтения» с классификационной меткой, равной нулю (0), в целях исключения влияния средств мандатного управления доступом ОС СН узла виртуализации на маркировку сетевых пакетов, выполненную средствами защиты информации ОС виртуальной машины. Управление виртуальными машинами и доступ к файлу образа ВМ должно предоставляться уполномоченным

пользователям только с помощью средств управления виртуализации.

Особенности настройки и применения любого из перечисленных способов приводятся в эксплуатационной документации на автоматизированную систему и/или отдельной инструкции по защите информации, подлежащих согласованию с подразделением, ответственным за защиту информации

3.2.4. На одном узле виртуализации рекомендуется настраивать ВМ одного уровня конфиденциальности.

3.2.5. Не допускается использование программного многоуровневого коммутатора Open vSwitch.

3.2.6. Не рекомендуется использование гостевого агента QEMU на ненулевом уровне конфиденциальности.

4. ОПИСАНИЕ ЗАДАЧИ

Основная задача, решаемая ПК СВ в процессе функционирования, — создание виртуальной среды в ОС СН. При этом возможны два режима работы ПК СВ:

1) сервисный режим — все ВМ запускаются от имени служебного пользователя системы (`oneadmin`). Авторизацию в веб-интерфейсе ПК СВ обеспечивает PAM-модуль службы `apache2`;

2) дискреционный режим — предназначен для создания защищенной виртуальной среды, в которой обеспечивается дискреционное и мандатное управление доступом к облаку ресурсов и виртуальных машин. В таком режиме ВМ запускаются от имени доменного пользователя, авторизовавшегося в ПК СВ. Для работы в дискреционном режиме необходимо, чтобы все серверы, на которых развернуто облако ресурсов и виртуальных машин, входили в один домен FreeIPA.

4.1. Ограничения функциональности, связанные с работой СЗИ

При выборе дискреционного режима работы ПК СВ следует учитывать следующие ограничения функциональности, связанные с работой СЗИ из состава ОС СН:

- при использовании ВМ с ненулевым мандатным контекстом, использование протокола ssh невозможно (ssh не работает под уровнем > 0);
- при использовании ВМ с ненулевым мандатным контекстом в качестве сетевого адаптера не может быть выбрано устройство virtio;
- в облачной сети, при выборе режима работы Open vSwitch, не поддерживаются классификационные метки, таким образом этот сетевой режим может использоваться только на минимальном уровне конфиденциальности;
- файловая система NFS в NAS не поддерживает файловые атрибуты безопасности, поэтому использование данной ФС при построении облачного хранилища недопустимо;
- в случае использования в качестве гостевой системы ОС СН, виртуальная машина не должна запускаться в мандатном контексте. Вместо этого необходимо выполнять удаленный вход с требуемым мандатным уровнем доступа средствами ОС СН.

4.2. Классы решаемых задач

Для решения основной задачи функционирования ПК СВ она делится на следующие классы задач:

- управление виртуальными машинами (4.2.1);
- идентификация и аутентификация при доступе к сервису фронтальной машины (4.2.2);

- идентификация и аутентификация при доступе к рабочему столу виртуальных машин (4.2.3);
- дискреционное и мандатное управление доступом к ВМ (только в дискреционном режиме работы ПК СВ) — 4.2.4.

4.2.1. Управление виртуальными машинами

Управление виртуальными машинами в ПК СВ осуществляется с помощью сервиса фронтальной машины из состава ПК СВ, который предоставляет средства создания и учета виртуальных машин, настройки их конфигурации и непосредственно запуска. В эти задачи входит управление файлами-образов дисковых носителей виртуальных машин, виртуальными сетевыми адаптерами и сетями и формирование контекста функционирования виртуальной машины в виде процесса ОС СН.

Для хранения конфигурации и параметров виртуальных машин используются шаблоны ВМ — описания конфигурации виртуальных машин. В файле конфигурации задается состав аппаратных средств, которые необходимо эмулировать для данной виртуальной машины, а также параметры использования ресурсов сервера виртуализации (процессора, оперативной памяти и других физических устройств).

Для взаимодействия пользователя с сервисом фронтальной машины в части касающейся управления ВМ используются инструменты командной строки и веб-интерфейс ПК СВ, описание которых приведено в документе в документе «Программный комплекс «Средства виртуализации «Брест» (ПК СВ «Брест») РДЦП.10001-03. Руководство администратора. Часть 2».

4.2.2. Идентификация и аутентификация при доступе к сервису фронтальной машины

Пользователь в ПК СВ определяется по имени и паролю. Создавать новую учетною запись в ОС СН для каждого пользователя ПК СВ не требуется. Аутентификация пользователей ПК СВ осуществляется при помощи строки сессии в каждой операции, которая проверяется ядром ПК СВ (службой `oned`).

Каждый пользователь обладает уникальным идентификатором и принадлежит к группе.

При первом запуске ПК СВ автоматически создаются следующие группы:

- `brestadmins` — администраторы ПК СВ, обладают полномочиями, чтобы выполнить любую операцию в отношении любого объекта. При этом в этой группе автоматически создаются следующие пользователи:
  - `oneadmin` — используется для взаимодействия всех систем ПК СВ,
  - `serveradmin` — используется сервисом веб-интерфейса ПК СВ для взаимо-

действия с другими сервисами ПК СВ;

- `brestusers` — пользователи инфраструктуры, имеют доступ к большей части функционала, предлагаемого ПК СВ для управления ресурсами.

Кроме того, при инициализации сервиса фронтальной машины в ПК СВ создается пользователь группы администраторов ПК СВ:

- в сервисном режиме функционирования ПК СВ — пользователь `brestadmin`;
- в дискреционном режиме функционирования ПК СВ — доменный пользователь, имя которого указывается вручную при инициализации сервиса фронтальной машины.

Порядок управления пользователями в ПК СВ представлен в документе «Программный комплекс «Средства виртуализации «Брест» (ПК СВ «Брест») РДЦП.10001-03. Руководство администратора. Часть 2».

4.2.3. Идентификация и аутентификация при доступе к рабочему столу ВМ

В ПК СВ для доступа к рабочему столу виртуальных машин используется браузерный VNC/SPICE клиент (noVNC).

Параметры аутентификации при доступе к рабочему столу виртуальной машины задаются в конфигурационном файле `/etc/one/sunstone-server.conf`. В данном конфигурационном файле указываются необходимые параметры аутентификации и пути к файлам сертификата и ключа. Используемые по умолчанию настройки представлены ниже.

```
:vnc_proxy_port: 29876
:vnc_proxy_support_wss: only
:vnc_proxy_cert: /etc/one/ssl/one-apache2.crt
:vnc_proxy_key: /etc/one/ssl/one-apache2.key
:vnc_proxy_ipv6: false
:vnc_request_password: false
:allow_vnc_federation: no
```

По умолчанию в ПК СВ устанавливается защищенной соединение на порт 29876, при этом используется самоподписанный SSL-сертификат.Подключение доступно только по протоколу IPv4. При подключении пароль не запрашивается. В случае объединения различных экземпляров ПК СВ, например развернутых в географически разнесенных центрах обработки данных (федерация), кнопка для запуска VNC/SPICE клиента в веб-интерфейсе не отображается.

4.2.4. Дискреционное и мандатное управление доступом к ВМ

ВНИМАНИЕ! Дискреционное и мандатное управление доступом к ВМ возможно только в дискреционном режиме работы ПК СВ.

Для настройки мандатного контроля целостности, дискреционного и мандатного управления доступом виртуальной машины необходимо в веб-интерфейсе ПК СВ на страни-

це этой ВМ открыть вкладку **Безопасность** и выполнить следующие действия (см. рис. 2.):

- в секции **Модель PARSEC** в выпадающем списке **Тип** выбрать тип модели мандатного управления доступом (динамический или статический). При выборе статического типа модели в поле **Метка** необходимо задать мандатную метку;
- в секции **Дискреционный контроль доступа** следует:
  - в выпадающем списке **Тип** выбрать тип субъекта (пользователь или группа);
  - в выпадающем списке **Субъект** выбрать соответствующего субъекта (пользователя или группу);
  - в выпадающем списке **Права доступа** выбрать типа доступа к виртуальной машине:
    - «Управление» — разрешен полный доступ к ВМ, включая запуск, правку ее свойств и управление правами доступа к ней;
    - «Использование» — разрешен только просмотр свойств, запуск и работа с виртуальной машиной.

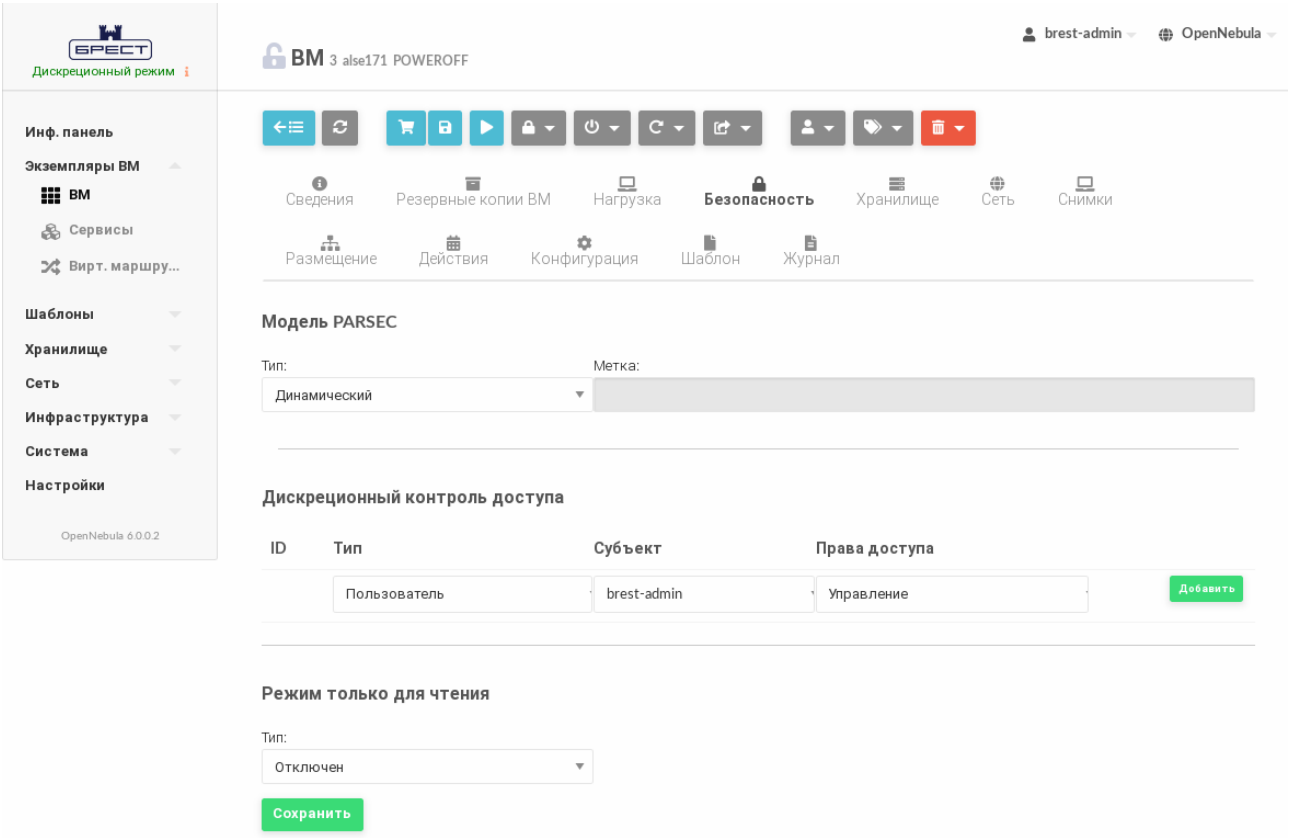

Рис. 2

ВНИМАНИЕ! Дискреционное и мандатное управление доступом к ВМ осуществляются СЗИ из состава ОС СН.

5. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входными данными ПК СВ являются:

- сведения о программно-аппаратной конфигурации оборудования сервера, на котором развернут сервис узла виртуализации и возможностях эмуляции аппаратного обеспечения виртуальных машин. Данные сведения собираются системой мониторинга в процессе своего функционирования путем запуска тестовых программ. Собранные данные используются в дальнейшем при создании и запуске виртуальных машин;
- шаблоны ВМ. Конфигурационные параметры, содержащиеся в данных шаблонах, отвечают за различные аспекты функционирования виртуальных машин: интерфейсы взаимодействия и права доступа к ним, способы и параметры аутентификации, политику управления безопасностью и изоляцией виртуальных машин, значения по умолчанию некоторых параметров конфигурации виртуальных машин, состав выводимой в журнал информации и т.п.;
- загрузочные ISO-образы установочных дисков. Установочные диски используются в процессе создания виртуальных машин для работы гостевых ОС и в процессе их функционирования для дополнения и обновления состава программных средств, установленных в гостевые ОС;
- запросы субъектов доступа к сервису фронтальной машины для управления виртуальными машинами. Сервис фронтальной машины предоставляет возможность удаленного управления узлом виртуализации по сети. Доступ к сервису фронтальной машины возможен как с помощью локальных инструментов командной строки, так и по сети посредство веб-интерфейса;
- запросы субъектов доступа к рабочим столам функционирующих виртуальных машин посредством VNC/SPICE клиента в веб-интерфейсе. По умолчанию в ПК СВ устанавливается защищенной соединение, при этом используется самоподписанный SSL-сертификат.

Выходными данными ПК СВ являются:

- описания конфигурации виртуальных машин, сохраняемые в каталоге СУБД из состава ПК СВ при создании виртуальной машины. В описании конфигурации задается состав аппаратных средств, которые необходимо эмулировать для данной виртуальной машины, а также параметры использования ресурсов узла виртуализации (процессора, оперативной памяти и других физических устройств);
- файлы-образов носителей, используемых виртуальными машинами. Формат файла-образа зависит от выбранного средства эмуляции аппаратного обеспечения.

В ПК СВ используются следующие форматы образов: `raw`-формат (является фактически представлением физического диска) и формат `qcow2` (собственный формат QEMU, поддерживающий возможности сжатия, использования снимков и другие дополнительные возможности). Кроме того, существует возможность конвертирования форматов образов других средств эмуляции аппаратного обеспечения (например, VirtualBox);

- файлы процесса функционирования виртуальных машин (файлы логирования): текущее состояние, сохраненные состояния виртуальных машин, снимки состояния виртуальных машин и служебная информация по блокировкам;
- результаты запросов субъектов доступа к серверу виртуализации, передаваемые консольным и графическим интерфейсам управления виртуальными машинами;
- информация, снимаемая с эмулируемых устройств вывода информации виртуальных машин и передаваемая пользователю по протоколам VNC и SPICE (например, изображения рабочих столов);
- журнал регистрации событий ПК СВ, содержащий детальную информацию по всем действиям субъектов доступа по управлению виртуальными машинами.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ВМ — виртуальная машина

ОС — операционная система

ОС СН — операционная система специального назначения «Astra Linux Special Edition»

ПК СВ — программный комплекс «Средства виртуализации «Брест»

СЗИ — средства защиты информации

ФС — файловая система

ЦП — центральный процессор

FreeIPA — Free Identity, Policy and Audit (система централизованного управления идентификацией пользователей, задания политик доступа и аудита для сетей на базе Linux)

KVM — Kernel-based Virtual Machine (программное решение, обеспечивающее виртуализацию в среде Linux на платформе, которая поддерживает аппаратную виртуализацию на базе Intel VT (Virtualization Technology) либо AMD SVM (Secure Virtual Machine))

LVM — Logical Volume Manager (менеджер логических томов)

NFS — Network File System (сетевая файловая система)

NAS — Network Attached Storage (сетевая система хранения данных)

QEMU — Quick Emulator (средства эмуляции аппаратного обеспечения)

SASL — Simple Authentication and Security Layer (простая аутентификация и слой безопасности)

SPICE — Simple Protocol for Independent Computing Environments (простой протокол для независимой вычислительной среды)

SSH — Secure Shell Protocol (протокол передачи информации в зашифрованном виде)

SSL — Secure Sockets Layer (уровень защищенных сокетов — криптографический протокол, обеспечивающий защищенную связь)

VDI — Virtual Desktop Infrastructure (инфраструктура виртуальных рабочих столов)

VLAN — Virtual Local Area Network (виртуальная локальная вычислительная сеть)

VNC — Virtual Network Computing (система удаленного доступа к рабочему столу компьютера)

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					
1		Все				РДЦП.01-18			20.08.18
2		Все				РДЦП.02-18			21.08.18
3		Все				РДЦП.01-19			16.05.19
4		Все				РДЦП.03-19			11.11.19
5		Все				РДЦП.02-20			06.07.20
6		Все				РДЦП.04-21			01.12.21