Утвержден

РДЦП.10001-02-УД

ПРОГРАММНЫЙ КОМПЛЕКС «СРЕДСТВА ВИРТУАЛИЗАЦИИ «БРЕСТ»

Описание применения

РДЦП.10001-02 31 01

Листов 21

2023

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 управления средой виртуализации, создание и защита которой обеспечивается средствами операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 очередное обновление 1.7 (далее по тексту — ОС СН).

1.2. Область применения

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

1.3. Возможности

ПК СВ предоставляет следующие возможности:

- создание ВМ, их образов и шаблонов;
- формирование среды выполнения ВМ;
- управление конфигурацией ВМ с помощью графического и консольного интерфейсов;
- централизованное управление средой виртуализации.

ПК СВ функционирует только под управлением операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 очередное обновление 1.7 (далее по тексту — ОС СН), имеющей сертификат соответствия ФСТЭК России № 2557, и совместно с ней обеспечивает выполнение следующих функций безопасности информации в соответствии с требованиями по безопасности информации к средствам виртуализации[1)] :

- доверенная загрузка виртуальных машин;
- контроль целостности;
- регистрация событий безопасности;
- управление доступом;
- резервное копирование;
- управление потоками информации;
- защита памяти;
- ограничение программной среды;
- идентификация и аутентификация пользователей.

Функция централизованного управления (администрирование) ВМ и взаимодействием между ними реализуется собственными средствами изделия.

ПК СВ интегрирован с комплексом средств защиты информации ОС СН и дополнительно обеспечивает выполнение следующих функций безопасности:

[1)] Утверждены приказом ФСТЭК России от 27.10.2022 № 187.

- дискреционное и мандатное управление доступом к ВМ и образам ВМ, в том числе при межпроцессном и сетевом взаимодействии, включая взаимодействие между ВМ по протоколам стека IPv4 и IPv6 в условиях мандатного управления доступом и доступ субъектов к файлам-образам и экземплярам функционирующих ВМ;
- создание кластеров высокой доступности с общим хранилищем, обеспечивающих отказоустойчивое функционирование ВМ посредством миграции ВМ между узлами кластера;
- обновление программного обеспечения изделия с использованием штатных средств ОС СН.

Реализация перечисленных функций безопасности основана на основных положениях, изложенных в документе РДЦП.10001-02 97 01 «Программный комплекс «Средства виртуализации «Брест». Руководство по КСЗ».

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. Требования к среде функционирования

ПК СВ функционирует только под управлением ОС СН на максимальном уровне защищенности («Смоленск») или усиленном уровне защищенности («Воронеж»). При этом допускается развертывание ПК СВ в сервисном режиме на компьютерах под управлением ОС СН, функционирующей на базовом уровне защищенности («Орел»).

Для обеспечения корректного функционирования ПК СВ необходимо установить программное обеспечение оперативных обновлений ОС СН бюллетень № 2023-0426SE17 (оперативное обновление 1.7.4) и бюллетень № 2023-0630SE17MD (оперативное обновление 1.7.4.UU.1).

Примечание. Допускается сразу устанавливать оперативное обновление 1.7.4.UU.1 без предварительной установки оперативного обновления 1.7.4.

После установки оперативного обновления рекомендуется применение ядра `linux-5.15-generic`.

2.2. Требования к техническим средствам

2.2.1. Обзор архитектуры

ПК СВ может функционировать в двух режимах:

1) в сервисном режиме все ВМ запускаются от имени непривилегированного пользователя. Идентификация и аутентификация пользователей основываются на использовании механизма PAM, реализованного в ОС СН. При этом аутентификация осуществляется с помощью локальной БД пользователей (файл /etc/passwd) и локальной БД пользовательских паролей (файл /etc/shadow);

2) в дискреционном режиме обеспечивается функционирование защищенной среды виртуализации, в том числе дискреционное и мандатное управление доступом к ВМ. В таком режиме ВМ запускаются от имени доменного пользователя, авторизовавшегося в ПК СВ. Для работы в дискреционном режиме необходимо, чтобы все компьютеры, на которых развернуты программные компоненты ПК СВ, входили в один домен FreeIPA.

Режим функционирования устанавливается на этапе развертывания ПК СВ. После установки и инициализации программных компонент переключение режимов функционирования ПК СВ не предусмотрено.

Создание и защита среды виртуализации обеспечиваются встроенными средствами ОС СН, интегрированными с подсистемой безопасности PARSEC, предназначенной для реализации функций ОС СН по защите информации от несанкционированного доступа:

- модулем ядра KVM, который использует аппаратные возможности архитектуры x86-64 по виртуализации процессоров;
- средствами эмуляции аппаратного обеспечения на основе QEMU;
- сервером виртуализации на основе libvirt.

В ПК СВ входят следующие программные компоненты серверной части:

- сервер виртуализации — для возможности создания виртуальных машин посредством эмуляции аппаратного обеспечения;
- сервер управления — для возможности управления через веб-интерфейс, из командной строки (консольный интерфейс) и с помощью XML-RPC API.

В качестве клиентской части изделия может выступать средство вычислительной техники, с которого выполняется подключение к серверу управления или виртуальной машине (ВМ).

В качестве дополнительных программных компонентов (не входят в состав ПК СВ) выступают:

- хранилище — 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 или nfs);
  - блочной технологии хранения с использованием LVM;
  - программно-определяемой технологии хранения Ceph;
- контроллер домена — служба, обеспечивающая аутентификацию пользователей в рамках единого пространства пользователей (не используется в сервисном режиме работы ПК СВ).

Примечание. В ПК СВ в качестве службы управления единым пространством пользователей используется FreeIPA из состава ОС СН. Если на объекте эксплуатации уже имеется настроенный домен FreeIPA, то разворачивать дополнительный контроллер домена нет необходимости. Все серверы вводятся в существующий домен.

ПК СВ может быть развернут как на группе компьютеров, так и на виртуальных машинах в пределах одного компьютера для тестирования. Для объединения компьютеров, обеспечения выполнения операций управления и поддержки виртуальных сетей используется локальная сеть.

Примечание. Допускается разворачивать несколько программных компонент ПК СВ на одном компьютере.

ВНИМАНИЕ! В связи с особенностью функционирования домена FreeIPA, конфигурация, при которой разворачиваются контроллер домена и служба сервера управления на одном компьютере, недопустима.

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

В 2.2.2–2.2.3 приведены основные требования к техническим средствам, на которых планируется развернуть 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.

2.2.2. Требования сервера управления

Минимальные рекомендуемые характеристики компьютера для развертывания службы сервера управления 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 виртуализации (компьютеров, на которых установлена и инициализирована служба сервера виртуализации), которым можно управлять с помощью одного экземпляра сервера управления, зависит от производительности и масштабируемости инфраструктуры ПК СВ и главным образом от системы хранения данных. Не рекомендуется использовать один экземпляр сервера управления для управления более чем 500 серверами виртуализации.

Сервер управления (компьютер, на котором установлена и инициализирована служба сервера управления) должен иметь сетевое соединение со всеми серверами виртуализации и, по возможности, доступ к хранилищам данных (как локальным, так и сетевым). Для обеспечения надежности инфраструктуры ПК СВ рекомендуется использовать как минимум две сети (соответственно, требуется два сетевых интерфейса):

1) сервисная сеть — используется службой сервера управления для обеспечения доступа к серверам виртуализации с целью управления и мониторинга гипервизоров и перемещения файлов образов;

2) сеть экземпляров — обеспечивает возможность сетевого подключения к виртуальным машинам через различные серверы виртуализации.

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

Для базовой установки службы сервера управления требуется не более 150 МБ.

2.2.3. Требования сервера виртуализации

Минимальные рекомендуемые характеристики компьютера для развертывания службы сервера 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, потребуются 80 физических ЦП. При этом 80 физических ЦП могут распределяться по различным серверам виртуализации: 10 компьютеров с восемью ядрами каждый или пять компьютеров 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 ПК СВ отсутствует избыточно выделяемая память. Как правило, рекомендуется всегда предусматривать резерв 10 % по ресурсам, потребляемым гипервизором. Например, для нагрузки в 40 виртуальных машин с 2 ГБ оперативной памяти каждая необходимо около 90 ГБ физической памяти (с учетом ресурса оперативной памяти, потребляемой гипервизором). Например, пять компьютеров с 24 ГБ оперативной памяти каждый предоставят по 22 ГБ памяти, поэтому они смогут выдержать планируемую нагрузку;

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

В каждом сервере виртуализации в зависимости от конфигурации хранилища и сети может 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».

Эксплуатация изделия должна осуществляться с учетом условий и указаний, установленных в документе РДЦП.10001-02 97 01.

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

2.4. Порядок обновления

В целях обеспечения соответствия требованиям безопасности информации в части устранения недекларированных возможностей и уязвимостей осуществляется ее техническая поддержка, предусматривающая выпуск очередного и оперативного обновлений.

Порядок выпуска и доведения обновлений до потребителей установлен в настоящем документе.

Информирование потребителей об окончании производства и (или) поддержки безопасности осуществляется с использованием контактной информации, указанной в заключенных ранее лицензионных договорах (дополнениях к лицензионным договорам) и путем размещения соответствующей информации на сайте изготовителя. Информирование ФСТЭК России — официальным почтовым сообщением не позднее чем за один год до окончания производства и (или) поддержки безопасности ПК СВ.

2.4.1. Очередное обновление

Очередное обновление представляет собой заводские экземпляры ПК СВ, изготовленные в соответствии с конструкторской (программной) и технологической документацией, действующей на момент изготовления, с внесенными в нее порядком, установленным ГОСТ 2.503-2013, плановыми изменениями.

Очередное обновление решает следующий комплекс задач:

1) устранение критических и некритических уязвимостей;
2) обеспечение усовершенствования (модернизации) конструкции;
3) поддержка современного оборудования;
4) реализация новых функциональных возможностей;
5) обеспечение соответствия актуальным требованиям безопасности информации;
6) повышение удобства использования, управления компонентами ПК СВ и другие.

Очередное обновление предоставляется пользователям при заключении соответствующего лицензионного договора или дополнения к имеющемуся лицензионному договору, а также в соответствии с положениями «Лицензионного соглашения с конечным пользователем по использованию операционной системы специального назначения «Astra Linux Special Edition». Информация о выпуске очередного обновления ОС размещается на официальном сайте изготовителя, а также доводится до лицензиатов (потребителей) с использованием контактной информации, указанной в заключенных ранее лицензионных договорах (дополнениях к лицензионным договорам).

Контроль целостности очередного обновления проводится следующим порядком:

- до установки — проведением проверки электронной подписи изготовителя (только для способа распространения по сетям связи);

- до установки — путем подсчета контрольной суммы установочного диска ПК СВ из комплекта поставки и сравнения с контрольной суммой, указанной в формуляре;
- после установки обновления — контроль целостности файлов программного обеспечения ПК СВ путем подсчета контрольных сумм файлов утилитой `fly-admin-int-check` с применением файла `gostsums.txt`, расположенного в корневом каталоге образа установочного диска (образа установочного диска).

В целях поддержания информационных (автоматизированных) систем в безопасном состоянии, обеспечения их работоспособности совместно с современным оборудованием и увеличения срока эксплуатации, рекомендуется на постоянной основе планировать и организовывать проведение мероприятий по применению очередного обновления ПК СВ.

2.4.2. Оперативное обновление

Оперативное обновление решает задачи:

1) оперативного устранения критических уязвимостей и уязвимостей высокого уровня опасности[1)] в экземплярах ПК СВ, находящихся в эксплуатации;
2) устранения функциональных недостатков;
3) совершенствование функциональных возможностей;

и представляет собой бюллетень безопасности, который может быть доступен в виде:

1) инструкций и методических указаний по настройке и особенностям эксплуатации ПК СВ, содержащих сведения о компенсирующих мерах или ограничениях по применению ПК СВ при эксплуатации;
2) отдельных программных компонентов из состава ПК СВ, в которые внесены изменения с целью устранения уязвимостей, инструкций по их установке и настройке, а также информации, содержащей сведения о контрольных суммах всех файлов оперативного обновления;
3) обновлений безопасности, представляющих собой файл с совокупностью программных компонентов из состава ПК СВ, в которые внесены изменения с целью устранения уязвимостей, а также информации, содержащей сведения о контрольных суммах всех файлов обновлений безопасности, указания по установке, настройке и особенностям эксплуатации ПК СВ с установленными обновлениями безопасности.

Обновления безопасности представляют собой отдельные программные документы, не предусматривающие внесения изменений в комплект документации очередного обновления, характеристики которого подтверждены сертификатом соответствия требованиям безопасности информации. Таким образом, сертификат соответствия очередного обновления ПК СВ, поставляемого потребителям в комплектности в соответствии с формуляром, является действующим вне зависимости от выпуска оперативного обновления.

[1)] В соответствии с ГОСТ Р 56545-2015.

Оперативное обновление содержит информацию об устраненных уязвимостях и предоставляется пользователям на безвозмездной основе.

Лицензиаты (потребители) оповещаются о выпуске и возможности получения обновления с использованием контактной информации, указанной в лицензионных договорах и дополнениях к ним, путем размещения соответствующей информации на официальном сайте и через личный кабинет.

Оперативное обновление не является самостоятельным программным изделием. Серийное производство и поставка (в том числе на материальных носителях) оперативного обновления не предусмотрены.

Доведение оперативного обновления до потребителей осуществляется изготовителем путем распространения по сетям связи. Источником получения оперативного обновления, подписанного усиленной квалифицированной электронной подписью изготовителя, является официальный сайт изготовителя.

Перед применением оперативного обновления необходимо учесть сведения о его совместимости с обновлениями ОС СН с использованием информации, указанной в бюллетене и на официальном справочном ресурсе `wiki.astralinux.ru/brest`.

Контроль целостности оперативного обновления и программного обеспечения ПК СВ после применения обновления осуществляется следующим порядком:

1) до установки обновления — путем проверки электронной подписи программного обеспечения обновления (образа установочного диска обновления или файлов, содержащих программное обеспечение с внесенными изменениями);

2) до установки обновления — проведением контроля целостности образа установочного диска оперативного обновления (или файлов, содержащего программное обеспечение с внесенными изменениями) путем подсчета его контрольной суммы и сравнения с контрольной суммой, указанной в бюллетене;

3) после установки обновления — проведением контроля целостности с использованием функции хэширования и автоматической сверки полученного значения с эталонным, указанным в специальном файле `gostsums.txt` с контрольными суммами, входящем в состав оперативного обновления.

В рамках аттестации или при реализации мер по обеспечению целостности (меры группы «ОЦЛ») информационных систем, функционирующих с применением ПК СВ, в целях подтверждения целостности, подлинности и неизменности сертифицированного программного обеспечения необходимо:

- проверить указание номера бюллетеня, содержащего оперативное обновление, в разделе «Сведения о бюллетенях» формуляра ПК СВ;
- контроль целостности установочного диска проводится путем подсчета контроль-

ной суммы установочного диска ПК СВ из комплекта поставки и сравнения с контрольной суммой, указанной в формуляре;

- контроль целостности файлов программного обеспечения ПК СВ после применения оперативного обновления путем подсчета контрольных сумм файлов утилитой `fly-admin-int-check` с применением файла `gostsums.txt`, расположенного в корневом каталоге образа установочного диска (образа установочного диска).

3. ОПИСАНИЕ ЗАДАЧИ

Основная задача, решаемая ПК СВ в процессе функционирования, — управление средой виртуализации, создание и защита которой обеспечивается средствами ОС СН.

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

1) создание ВМ, их образов и шаблонов;
2) формирование среды выполнения ВМ;
3) управление конфигурацией ВМ с помощью графического и консольного интерфейсов;
4) централизованное управление средой виртуализации;
5) защита среды виртуализации.

Для решения указанных классов задач ПК СВ предоставляет следующие возможности:

1) создание виртуальных машин, их образов и шаблонов с помощью графического и консольного интерфейсов с поддержкой 32 и 64-битных гостевых операционных систем (ОС):
   - 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 соответствующей инфраструктуры серверов);
   - создание ВМ из настраиваемых шаблонов (возможность группового создания 500 и более ВМ из шаблонов);
2) управление конфигурацией ВМ с помощью графического и консольного интерфейсов;
3) администрирование средств виртуализации:
   - 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;
   - изменение без завершения функционирования ВМ количества выделенных им процессоров и размера оперативной памяти;

- добавление виртуальных дисков в гостевую операционную систему и увеличение их размеров без остановки ВМ;
- подключение к ВМ устройств PCI и USB, включая USB 3.0, из состава аппаратных средств, на которых функционирует серверная часть изделия;
- удаленное подключение к ВМ по протоколу SPICE USB-устройств из состава аппаратных средств клиентской части изделия;
- управление приоритетом дисковых операций ввода-вывода для ВМ;
- обеспечение возможности клонирования 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;
- обслуживание узла в сервисном режиме с автоматическим перемещением работающих ВМ без их остановки;

4) обеспечение возможности централизованного хранения конфигурационной информации о ВМ и среде виртуализации;

5) обеспечение возможности создания копий трафика виртуальных машин внутри виртуального сетевого коммутатора на его сетевой порт;

6) обеспечение возможности создания резервных копий виртуальных машин, а также их последующего восстановления;

7) обеспечение поддержки виртуальных коммутаторов с технологией VLAN (Virtual Local Area Network);

8) обеспечение возможности централизованного управления кластерами, серверной частью изделия на всех узлах кластера высокой доступности, хранилищами и виртуальными коммутаторами;

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

10) обеспечение мониторинга работоспособности и использования ресурсов виртуальными машинами и серверной частью изделия и генерации отчетов, в т.ч. за выбранный период;

11) поддержка серверной частью изделия следующих механизмов оптимизации оперативной памяти: дедупликация страниц, динамическое распределение, выгрузка

в файл подкачки;

12) обеспечение отказоустойчивого функционирования системы управления: создание кластеров высокой доступности, обеспечивающих отказоустойчивое функционирование ВМ посредством репликации файлов ВМ между системами хранения и миграции ВМ между узлами кластера;

13) предоставление графического интерфейса управления пользователями и их группами;

14) создание облачных хранилищ;

15) мониторинг и учет информации, касающейся узлов виртуализации и ВМ;

16) возможность объединения нескольких экземпляров ПК СВ в единый центр обработки и хранения данных (ЦОХД).

Описание указанных функций приведено в документах РДЦП.10001-02 95 01-1 «Программный комплекс «Средства виртуализации «Брест». Руководство администратора. Часть 1» и РДЦП.10001-02 95 01-2 «Программный комплекс «Средства виртуализации «Брест». Руководство администратора. Часть 2».

Решение задач защиты среды виртуализации обеспечивается функциями безопасности в соответствии с Требованиями по безопасности информации к средствам виртуализации[1)]

1) доверенная загрузка виртуальных машин;

2) контроль целостности;

3) регистрация событий безопасности;

4) управление доступом;

5) резервное копирование;

6) управление потоками информации;

7) защита памяти;

8) ограничение программной среды;

9) идентификация и аутентификация пользователей;

10) централизованное управление (администрирование) ВМ и взаимодействием между ними;

Дополнительно задачи защиты среды виртуализации также обеспечиваются функциями:

1) дискреционное и мандатное управление доступом к ВМ и образам ВМ, в том числе при межпроцессном и сетевом взаимодействии, включая взаимодействие между ВМ по протоколам стека IPv4 и IPv6 в условиях мандатного управления доступом и доступ субъектов к файлам-образам и экземплярам функционирующих

[1)] Утверждены приказом ФСТЭК России от 27 октября 2022 г. № 187.

ВМ;

2) создание кластеров высокой доступности с общим хранилищем, обеспечивающих отказоустойчивое функционирование ВМ посредством миграции ВМ между узлами кластера;

3) обновление программного обеспечения изделия с использованием штатных средств ОС СН.

Описание указанных функций приведено в документе РДЦП.10001-02 97 01.

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входными данными ПК СВ являются:

1) сведения о программно-аппаратной конфигурации оборудования компьютера, на котором развернут служба сервера 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;

2) 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.;

3) 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;

4) запросы субъектов доступа к службе сервера управления. Служба сервера управления предоставляет возможность удаленного управления виртуальными машинами и службой сервера виртуализации по сети. Доступ к службе сервера управления возможен как с помощью локальных инструментов командной строки, так и по сети посредством веб-интерфейса;

5) 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:

1) описания конфигурации виртуальных машин, сохраняемые в СУБД PostgreSQL из состава ОС СН при создании виртуальной машины. В описании 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);

2) файлы образов дисков, 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);

3) файлы процесса функционирования виртуальных машин (файлы логирования): текущее состояние, сохраненные состояния виртуальных машин, снимки состояния виртуальных машин и служебная информация по блокировкам;

4) результаты запросов субъектов доступа к серверу виртуализации, передаваемые консольным и графическим интерфейсам управления виртуальными машинами;

5) информация, снимаемая с эмулируемых устройств вывода информации виртуальных машин и передаваемая пользователю по протоколам VNC и SPICE (например, изображения рабочих столов);

6) журнал регистрации событий, 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»

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)

QEMU — Quick Emulator (средства эмуляции аппаратного обеспечения)

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

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

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 сопро-водительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					
1		Все				РДЦП.01-18 от 20.08.2018			
2		Все				РДЦП.02-18 от 21.08.2018			
3		Все				РДЦП.01-19 от 16.05.2019			
4		Все				РДЦП.03-19 от 11.11.2019			
5		Все				РДЦП.02-20 от 06.07.2020			
6		Все				РДЦП.04-21 от 01.12.2021			
7		Все				РДЦП.02-22 от 22.07.2022			
8		Все				РДЦП.03-22 от 03.11.2022			
9		Все				РДЦП.06-23 от 22.09.2023			