Утвержден

РУСБ.10205-01-УД

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

ПК «ВИУ»

Описание применения

РУСБ.10205-01 31 01

Листов 21

2016

АННОТАЦИЯ

Настоящий документ является описанием применения программного комплекса виртуализации и управления (ПК «ВИУ») РУСБ.10205-01 (далее по тексту — ПК).

В документе описаны назначение ПК, условия его применения, описание задачи, также приведено описание входных и выходных данных ПК.

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1. Назначение

ПК предназначен для создания защищенной виртуальной среды, обеспечивающей функционирование виртуальных машин и управление ими в операционной системе специального назначения «Astra Linux Special Edition» РУСБ.10015-07 (далее по тексту — ОС СН) в условиях дискреционного и мандатного разграничения доступа.

1.2. Область применения

Автоматизированные системы в защищенном исполнении, обрабатывающие информацию ограниченного доступа, в том числе содержащую сведения, составляющие государственную тайну, со степенью секретности до «совершенно секретно» включительно.

1.3. Возможности

ПК предоставляет следующие возможности:

– обеспечение создания тонких (терминальных) клиентов с использованием технологии VDI (Virtual Desktop Infrastructure);

– использование аппаратных возможностей архитектуры x86-64 по виртуализации процессоров на основе модуля KVM (Kernel-based Virtual Machine) из состава ОС СН и средств эмуляции аппаратного обеспечения QEMU;

– идентификация и аутентификация пользователя до предоставления доступа к функциям виртуализации и управления ПК, в том числе в режиме взаимодействия со средствами создания единого пространства пользователей (ALD) из состава ОС СН;

– создание виртуальных машин с помощью графической и консольных утилит;

– запуск виртуальной машины в виде отдельного процесса ОС СН, который функционирует от имени учетной записи пользователя с его мандатными атрибутами безопасности;

– предоставление пользователям удаленного доступа к виртуальным машинам в соответствии с дискреционными и мандатными правилами разграничения доступа;

– управление конфигурацией виртуальных машин с помощью графической и консольных утилит;

– взаимодействие между виртуальными машинами по протоколам стека IPv4 в условиях мандатного разграничения доступа;

– взаимодействие между процессами пользователей и виртуальными машинами по протоколам стека IPv4 в условиях мандатного разграничения доступа;

– маршрутизация сетевых пакетов виртуальных машин;

– возможность защиты файлов-образов виртуальных машин от модификации в процессе функционирования виртуальных машин.

ПК обеспечивает реализацию следующих функций по защите информации от НСД:

– дискреционный принцип контроля доступа;
– мандатный принцип контроля доступа;
– очистку памяти;
– изоляцию модулей;
– маркировку документов;
– защиту ввода-вывода на отчуждаемый физический носитель информации;
– сопоставление пользователя с устройством;
– идентификацию и аутентификацию пользователей;
– регистрацию событий, связанных с работой СЗИ ПК;
– восстановление изделия после сбоев и отказов оборудования;
– контроль целостности комплекса средств защиты ПК.

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. Требования к программным средствам

ПК функционирует только под управлением ОС СН.

2.2. Требования к техническим средствам

Сервер и клиентское программное обеспечение ПК со встроенными СЗИ от НСД должны функционировать на оборудовании, отвечающему требованиям к аппаратному обеспечению под управлением ОС СН.

Для функционирования сервера виртуализации ПК необходима следующая минимальная конфигурация оборудования:

– аппаратная платформа — процессор с архитектурой x86-64 с аппаратной поддержкой виртуализации (AMD, Intel);
– оперативная память — от 8 ГБ;
– объем свободного дискового пространства — от 30 ГБ;
– сетевая плата 100 Мбит/с;
– источник бесперебойного питания;
– устройство чтения/записи CD/DVD-дисков.

3. ОПИСАНИЕ ЗАДАЧИ

Основная задача, решаемая ПК в процессе своего функционирования, — создание защищенной виртуальной среды в ОС СН.

3.1. Классы решаемых задач

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

– управление виртуальными машинами (3.2);

– идентификация и аутентификация при доступе к серверу виртуализации libvirt (3.3);

– идентификация и аутентификация при доступе к рабочему столу виртуальных машин (3.4);

– дискреционное управление доступом к виртуальным машинам (3.5);

– мандатное управление доступом к виртуальным машинам (3.6);

– функционирование виртуальной машины в режиме запрета модификации ее файлов-образов (3.7).

3.2. Управление виртуальными машинами

Управление виртуальными машинами в ПК осуществляется с помощью сервера виртуализации на основе libvirt, 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 xml файлы 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).

При создании виртуальной машины задаются конфигурационные параметры и создается файл-образ загрузочного диска виртуальной машины. Формат файла-образа зависит от выбранного средства эмуляции аппаратного обеспечения. В ПК используются средства эмуляции аппаратного обеспечения на основе QEMU, которые поддерживают следующие форматы образов: `image` (raw-формат, является фактически представлением физического диска) и формат `qcow2` (родной формат QEMU, поддерживающий возможности сжатия, использования снимков и другие дополнительные возможности). Кроме того, су-

ществует возможность конвертирования форматов образов других средств эмуляции аппаратного обеспечения (например, VirtualBox).

При запуске виртуальной машины сервер виртуализации libvirt подготавливает необходимую для функционирования виртуальной машины инфраструктуру и формирует соответствующий набор параметров запуска средства эмуляции аппаратного обеспечения QEMU. После подготовительных действий производится порождения процесса ОС СН, в рамках которого будет функционировать виртуальная машина. Каждая запускаемая виртуальная машина функционирует от имени учетной записи запустившего ее пользователя и с его мандатными атрибутами безопасности.

Для обеспечения безопасности функционирования виртуальных машин сервер виртуализации libvirt использует концепцию драйверов безопасности sVirt . Данная концепция представляет собой специальный программный интерфейс для создания модулей безопасности, используемых для настройки окружения и инфраструктуры запуска и функционирования виртуальный машин в условиях их изоляции и мандатного разграничения доступа.

Выполнение требований по защите информации при функционировании виртуальных машин в ОС СН достигается совместным использованием sVirt модуля дискреционного разграничения доступа `dac` и специально разработанного модуля мандатного разграничения доступа `parsec`, взаимодействующего с подсистемой безопасности PARSEC ОС СН.

На рис. 1 приведен снимок вкладки «Безопасность» графической утилиты управления виртуальными машинами `virt-manager`.

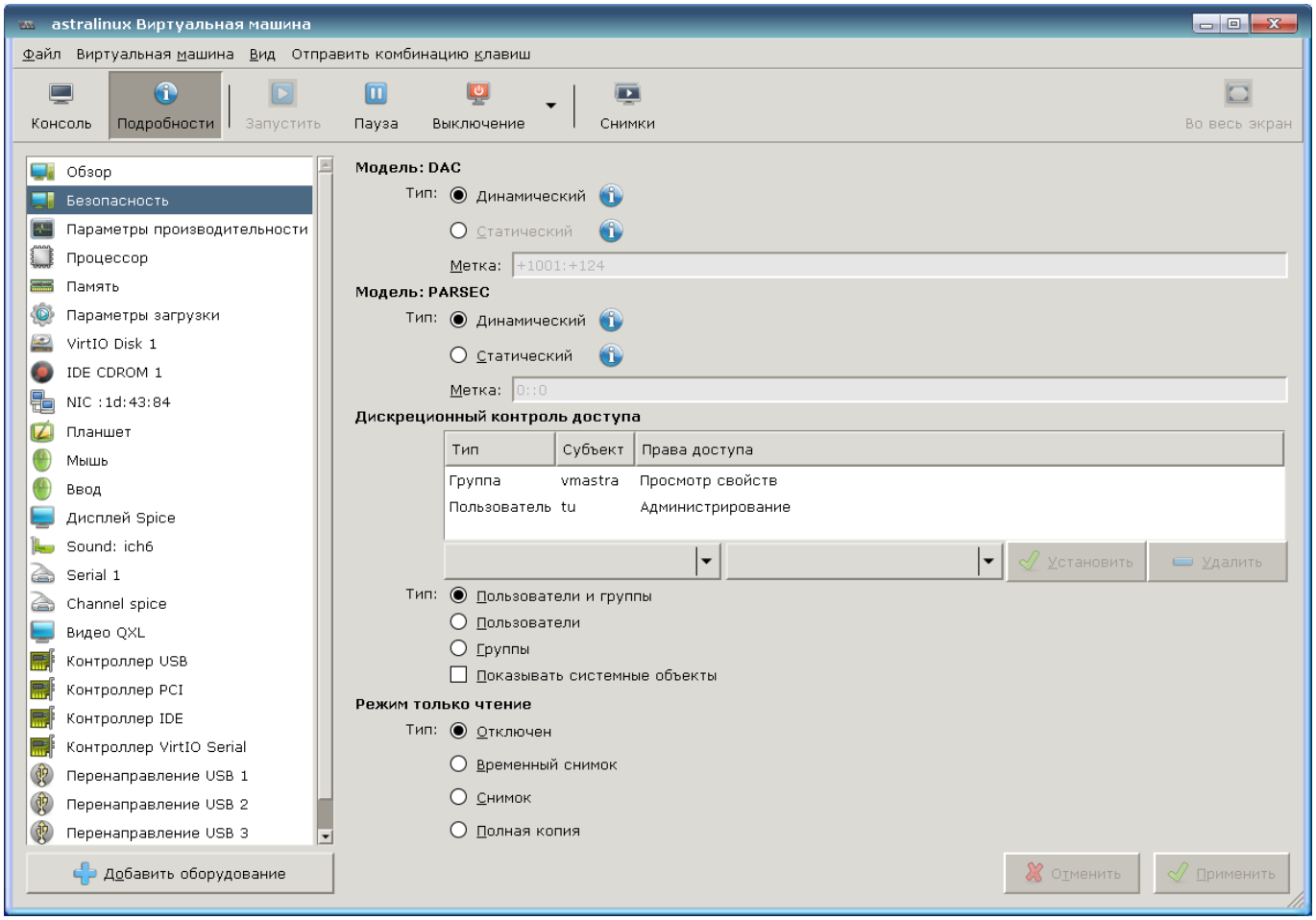

Рис. 1

Контекст безопасности виртуальной машины включает в себя метки безопасности используемых модулей sVirt, например:

– модуль поддержки дискреционного разграничения доступа `dac` использует метку безопасности, состоящую из уникального идентификатора владельца процесса виртуальной машины и уникального идентификатора группы;

– модуль поддержки мандатного разграничения доступа `parsec` использует мандатную метку подсистемы безопасности PARSEC ОС СН.

Метки безопасности могут быть динамическими и статическими:

– динамическая метка безопасности генерируется динамически в момент запуска виртуальной машины на основе атрибутов безопасности запускающего пользователя: его уникального идентификатора и мандатного уровня доступа;

– статическая метка безопасности задается администратором в конфигурации виртуальной машины определяет контекст безопасности ее запуска.

Поддержка дискреционного и мандатного управление доступом к виртуальным машинам в сервере виртуализации реализуется с помощью драйвера доступа `parsec`, специально разработанного с использованием прикладного программного интерфейса драйверов доступа libvirt. Подробное описание принципов управления доступом приведено в

следующих подразделах (см. 3.5 и 3.6).

Поддержка функционирования виртуальной машины в режиме запрета модификации ее файлов-образов осуществляется специальными способами запуска виртуальной машины, при которых основной файл-образ защищается от записи. В зависимости от выбранного режима используется создание физической копии или различные варианты создания снимков файл-образов с последующим их удалением после завершения работы виртуальной машины. Более подробно данный режим функционирования виртуальной машины описан в 3.7.

Рассматривая вопросы идентификации и аутентификации при доступе к виртуальным машинам следует различать доступ к серверу виртуализации libvirt для управления виртуальными машинами и доступ пользователя непосредственно к рабочему столу виртуальной машины.

3.3. Идентификация и аутентификация при доступе к серверу виртуализации libvirt

На рис. 2 приведен снимок диалогового окна задания параметров подключения к серверу виртуализации libvirt.

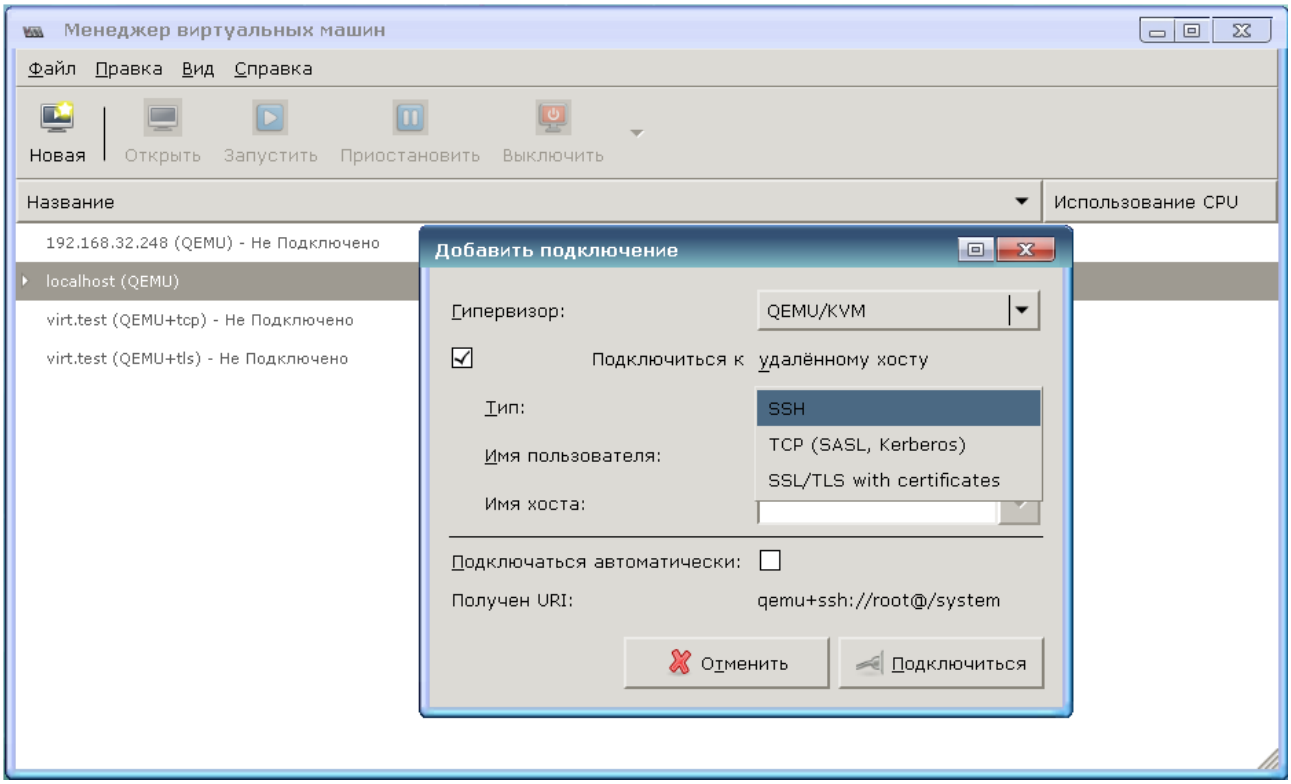

Рис. 2

Сервер виртуализации может использовать для идентификации и аутентификации клиентов следующие механизмы:

– локальная peer-cred аутентификация;

– удаленная SSH аутентификация (строка соединения `qemu+ssh://...`);

– удаленная SASL аутентификация в том числе с поддержкой Kerberos (строка соединения `qemu+tcp://...`);

– удаленная TLS аутентификация с использованием сертификатов (строка соединения `qemu+tls://...`).

Параметры аутентификации задаются в конфигурационном файле `/etc/libvirt/libvirtd.conf`. В конфигурационном файле отдельно задаются параметры для различных способов аутентификации: параметры локальных UNIX сокетов (секция «UNIX socket access control»), разрешение приема сетевых соединений (параметры `listen_tls` и `listen_tcp`) и порты для tcp и tls (параметры `tls_port` и `tcp_port`), расположение необходимых файлов при использовании сертификатов x509 (секция «TSL x509 certificate configuration») и варианты авторизации (параметры `auth_unix_ro`, `auth_unix_rw`, `auth_tcp`, `auth_tls`).

По умолчанию используется следующее расположение файлов сертификатов на сервере для аутентификации к серверу виртуализации libvirt:

– `/etc/pki/CA/cacert.pem` — корневой сертификат;

– `/etc/pki/CA/crl.pem` — файл отозванных сертификатов;

– `/etc/pki/libvirt/servercert.pem` — сертификат открытого ключа сервера виртуализации libvirt;

– `/etc/pki/libvirt/private/serverkey.pem` — закрытый ключ сервера виртуализации libvirt.

Примечание. Файлы ключей сервера виртуализации libvirt должны быть доступны на чтение группе `libvirt-qemu`.

По умолчанию используется следующее расположение файлов сертификатов на клиенте для аутентификации к серверу виртуализации libvirt (в домашнем каталоге пользователя ~):

– `/etc/pki/CA/cacert.pem` — корневой сертификат;

– `~/.pki/libvirt/clientcert.pem` — сертификат открытого ключа клиента;

– `~/.pki/libvirt/clientkey.pem` — закрытый ключ клиента.

В случае SASL аутентификации используется конфигурационный файл `/etc/sasl2/libvirt.conf`, в котором задаются параметры аутентификации SASL (например, применяемые механизмы). Имя сервиса сервера виртуализации libvirt при использовании SASL аутентификации регистрируется как `libvirt/<имя сервера>@<домен>`.

ВНИМАНИЕ! При указании механизма SASL `gssapi` следует в конфигурационном файле `/etc/default/libvirtd` указать с помощью соответствующей переменной окружения расположение файла ключей Kerberos сервера виртуализации, например:

`export KRB5_KTNAME=/etc/libvirt/libvirt.keytab`.

Примечание. Настройка сервера виртуализации для работы в ЕПП ОС СН производится в соответствием с документом РУСБ.10015-07 95 01 1 «Операционная система специального назначения «Astra Linux Special Edition Руководство администратора. Часть 1».

3.4. Идентификация и аутентификация при доступе к рабочему столу виртуальных машин

Параметры аутентификации при доступе к рабочему столу виртуальной машины задаются в конфигурационном файле `/etc/libvirt/qemu.conf` раздельно для протоколов VNC и Spice. В данном конфигурационном файле указываются необходимые параметры аутентификации и пути к конфигурационным файлам SASL, например `/etc/sasl2/qemu.conf`. Имя сервисов VNC и Spice при использовании SASL аутентификации регистрируется как `vnc/<имя сервера>@<домен>` и `spice/<имя сервера>@<домен>`, соответственно.

Примечание. Настройка сервисов VNC и Spice для работы в ЕПП ОС СН производится в соответствии с документом РУСБ.10015-07 95 01-1.

По умолчанию используется следующее расположение файлов сертификатов на сервере для аутентификации к виртуальной машине для по протоколу VNC:

– `/etc/pki/libvirt-vnc/ca-cert.pem` — корневой сертификат;

– `/etc/pki/libvirt-vnc/server-cert.pem` — сертификат открытого ключа сервера VNC QEMU;

– `/etc/pki/libvirt-vnc/server-key.pem` — закрытый ключ сервера VNC QEMU.

Примечание. Файлы ключей сервера VNC QEMU должны быть доступны на чтение группе `libvirt-qemu`.

По умолчанию используется следующее расположение файлов сертификатов на клиенте для аутентификации к серверу VNC QEMU (в домашнем каталоге пользователя ~):

– `/etc/pki/CA/cacert.pem` — корневой сертификат;

– `~/.pki/libvirt-vnc/clientcert.pem` — сертификат открытого ключа клиента;

– `~/.pki/libvirt-vnc/private/clientkey.pem` — закрытый ключ клиента.

3.5. Дискреционное управление доступом к виртуальным машинам

При взаимодействии с сервером виртуализации libvirt осуществляется дискреционное разграничение доступа к управлению виртуальными машинами.

Разграничение выполняется драйвером доступа `parsec`, специально разработанного с использованием прикладного программного интерфейса драйверов доступа libvirt.

Основанием для принятия решения о предоставлении доступа является сравнение дискреционных атрибутов виртуальной машины и дискреционных атрибутов пользователя с учетом выполняемой операции.

Все операции с виртуальной машиной разделяются на непривилегированные и привилегированные, например: операции получения информации о списке машин или о конфигурации конкретной машины являются операциями непривилегированными, а операции создания, удаления или изменения конфигурации виртуальных машин – привилегированными.

Операции по изменению состава или конфигурации виртуальных машин требуют вхождения пользователя в специальную локальную административную группу. Имя административной группы задается в конфигурационном файле `/etc/libvirt/libvirtd.conf` параметром:

```
admin_group = "libvirt-admin"
```

Для каждой виртуальной машины задается список контроля доступа, в котором указываются субъекты доступа (пользователи и группы), обладающие доступом к виртуальной машине. Различаются три типа доступа к виртуальной машине (см. рис. 3):

– «Просмотр свойств» — видимость виртуальной машины в списке и просмотр ее свойств;

– «Использование» — просмотр свойств, запуск и работа с виртуальной машиной;

– «Администрирование» — полный доступ к виртуальной машине, включая запуск, правку ее свойств и управление правами доступа к ней.

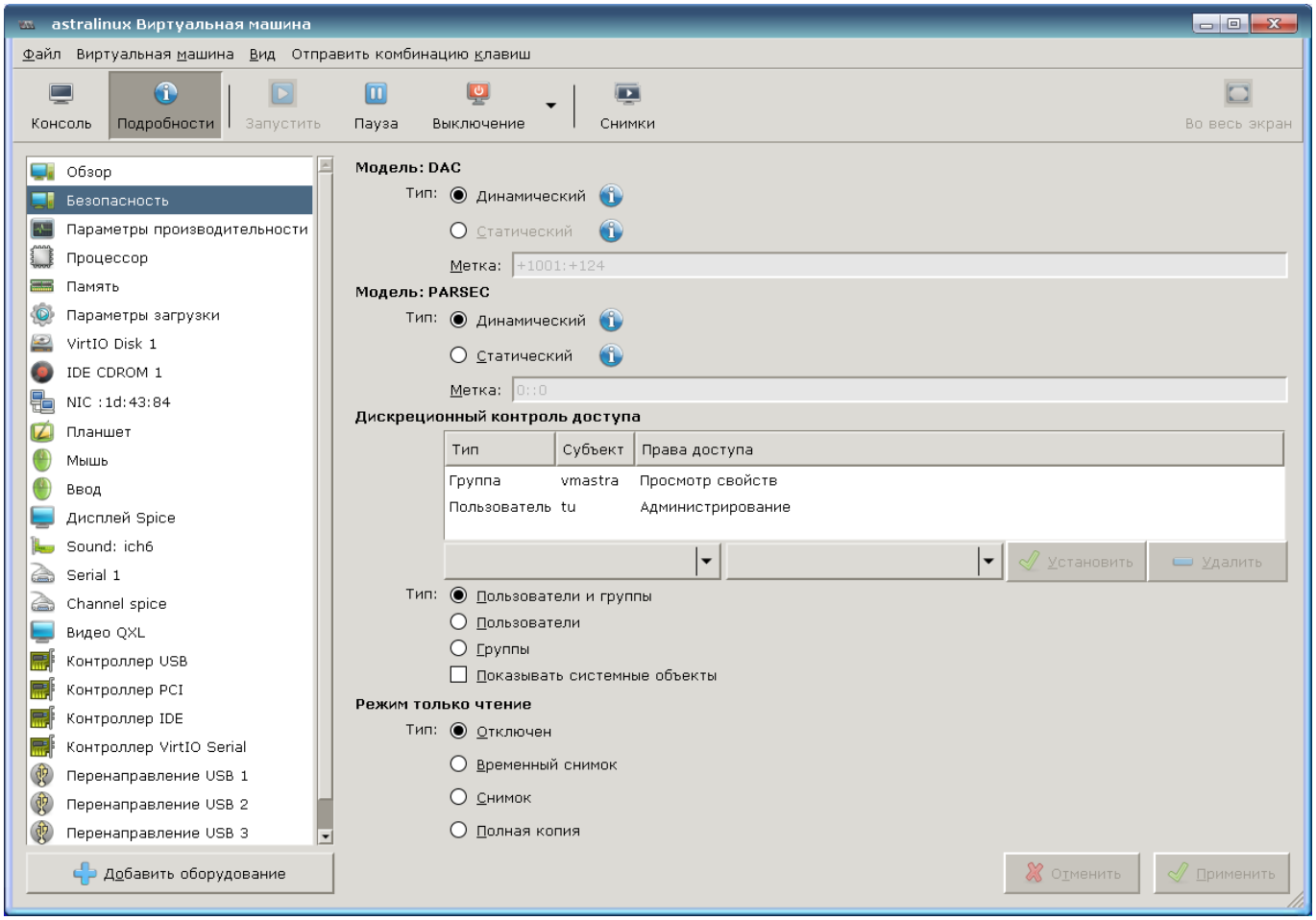

Рис. 3

Пользователи видят в списке виртуальных машин только те виртуальные машины, к которым им явно предоставлен доступ.

После создания виртуальной машины список контроля доступа пуст и доступ к виртуальной машине разрешен только членам административной группы. Пользователям, не входящим в административную группу, позволяется запускать виртуальные машины и работать с ними. При этом, завершить работу или произвести иные разрешенные действия с виртуальной машиной может только пользователь, который ее запустил. Члены административной группы могут завершать работу виртуальный машин других пользователей.

В момент запуска виртуальной машины модуль поддержки дискреционного разграничения доступа `dac` устанавливает виртуальной машине владельцем запускающего пользователя, а группой – группу `libvirt-qemu`. Это отражается в виде наличия динамической метки безопасности модели `DAC` и идентификатора владельца как процесса виртуальной машины в ОС СН, так и необходимых устройств и файл-образов, принадлежащих виртуальной машине. При последующих операциях эта информация используется для проверки дискреционного доступа к виртуальной машине.

3.6. Мандатное управление доступом к виртуальным машинам

При взаимодействии с сервером виртуализации libvirt осуществляется мандатное разграничение доступа к управлению виртуальными машинами.

Разграничение выполняется драйвером доступа `parsec`, специально разработанного с использование прикладного программного интерфейса драйверов доступа libvirt.

Основанием для принятия решения о предоставлении доступа является сравнение метки безопасности виртуальной машины и мандатного уровня доступа пользователя с учетом выполняемой операции.

Все операции с виртуальной машиной разделяются на операции чтения и записи, например: операции получения информации о списке машин или о конфигурации конкретной машины являются операциями чтения, а операции создания, удаления или изменения конфигурации виртуальных машин – записи. Мандатное разграничение доступа осуществляется следующим образом:

– остановленная виртуальная машина не обладает мандатными атрибутами (если для нее не задана статическая метка безопасности модели `PARSEC`);

– запущенная виртуальная машина наследует мандатную метку запускающего пользователя;

– доступ к функционирующей виртуальной машине предоставляется только при равенстве мандатного уровня доступа пользователя мандатной метке виртуальной машины;

– доступ к получению информации о виртуальной машине и ее конфигурации предоставляется в соответствии с мандатным уровнем пользователя.

В момент запуска виртуальной машины модуль поддержки мандатного разграничения доступа `parsec` устанавливает виртуальной машине мандатный уровень, определенный по соединению запускающего пользователя. Это отражается в виде наличия динамической метки безопасности модели `PARSEC` и мандатной метки как процесса виртуальной машины в ОС СН, так и необходимых устройств и файл-образов, принадлежащих виртуальной машине. При последующих операциях эта информация используется для проверки мандатного доступа к виртуальной машине.

Существует возможность задания статической метки безопасности модели `PARSEC`. В этом случае виртуальная машины может быть запущена только под заданным мандатным уровнем доступа.

ВНИМАНИЕ! Существуют ограничения по конфигурированию виртуальной машины: в качестве сетевого адаптера не может быть выбрано устройство `virtio`.

Примечание. 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.

Примечание. Настоятельно рекомендуется использовать режим «Только чтение» при запуске виртуальных машин в ненулевом мандатном контексте.

3.7. Функционирование виртуальной машины в режиме запрета модификации ее файлов-образов

В некоторых случаях требуется обеспечение неизменности файлов-образов виртуальной машины в процессе ее функционирования, что позволяет выполнять повторный запуск заранее подготовленных виртуальных машин из фиксированного состояния. В этом случае все результаты работы пользователя после завершения функционирования виртуальной машины удаляются.

В ПК такой режим работы называется «Режим только чтение» и достигается, как представлено на рис. 3, тремя разными способами:

– временный снимок — режим функционирования средства эмуляции аппаратного обеспечения QEMU, при котором основной файл-образ защищается от записи, а все результаты работы пользователя фиксируются во временном снимке, существующем только в процессе функционирования виртуальной машины;

– снимок — создание во время запуска виртуальной машины в заданном каталоге снимка, удаляемого после завершения функционирования виртуальной машины;

– полная копия — создание во время запуска виртуальной машины в заданном каталоге полной копии файла-образа, удаляемого после завершения функционирования виртуальной машины;

Вариант создания полной копии требует значительного времени запуска виртуальной машины за счет копирования файла-образа, который может обладать большим размером. Но данный вариант позволяет использовать возможности по сохранению состояния виртуальной машины для последующего его восстановления. При использовании снимков любое выключение виртуальной машины вследствие выключения или аппаратного сбоя сервера виртуализации, все результаты работы виртуальной машины будут потеряны.

Каталог размещения временных файлов задается в конфигурационном файле `/etc/libvirt/qemu.conf` следующим конфигурационным параметром:

```
run_images_dir = "/var/lib/libvirt/runimages"
```

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входными данными ПК являются:

– сведения о программно-аппаратной конфигурации оборудования сервера виртуализации и возможностях средства эмуляции аппаратного обеспечения на основе QEMU. Данные сведения собираются службой сервера виртуализации в процессе своего функционирования путем вызова внешних команд ОС и средства эмуляции. Собранные данные используются в дальнейшем при создании и запуске виртуальных машин;

– конфигурационные файлы службы сервера виртуализации и средства эмуляции аппаратного обеспечения на основе QEMU. Данные файлы расположены в каталоге `/etc/libvirt`. Конфигурационные параметры, содержащиеся в данных файлах, 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 или оптические диски с дистрибутивами гостевых ОС. 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 службе сервера виртуализации для управления виртуальными машинами. Служба сервера виртуализации `libvirtd` предоставляет возможность удаленного управления сервером виртуализации по сети с использованием различных протоколов и способов аутентификации. Доступ к службе сервера виртуализации возможен как с помощью локальных Unix-сокетов, так и по сети с помощью консольных или графических инструментов управления виртуальными машинами. В качестве способа аутентификации при использовании ПК в условиях ЕПП применяется аутентификация Kerberos с помощью механизма SASL `gssapi`, в иных случаях возможно применение других механизмов SASL или SSL/TLS аутентификации, основанной на сертификатах. Взаимодействие пользователей с сервером виртуализации состоит из обязательного прохождения процедуры аутентификации и работы в условиях применения дискреционных и мандатных правил разграничения доступа;

– запросы серверу виртуализации, передаваемые с помощью прикладного про-

граммного интерфейса (клиентской библиотеки). Для взаимодействия других программ с сервером виртуализации могут использоваться дополнительные программные интерфейсы из пакетов с префиксом `libvirt-`;

– запросы субъектов доступа к рабочим столам функционирующих виртуальных машин по протоколам VNC и Spice. Средства эмуляции аппаратного обеспечения на основе QEMU предоставляют интерфейсы доступа к рабочим столам функционирующих виртуальных машин по протоколам VNC и Spice, при этом применяются отдельные настройки аутентификации для каждого из протоколов. В качестве способа аутентификации при использовании ПК в условиях ЕПП применяется аутентификация Kerberos с помощью механизма SASL `gssapi`, в иных случаях возможно применение других механизмов SASL или SSL/TLS аутентификации, основанной на сертификатах.

Выходными данными ПК являются:

– XML-описания виртуальных машин, сохраняемые в каталоге `/etc/libvirt/qemu` при создании виртуальной машины. 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);

– файлы-образов носителей, используемых виртуальными машинами. Формат файлаобраза зависит от выбранного средства эмуляции аппаратного обеспечения. В ПК используются средства эмуляции аппаратного обеспечения на основе QEMU, которые поддерживают следующие форматы образов: image (raw-формат, является фактически представлением физического диска) и формат `qcow2` (родной 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 устройств хостовой ОС, создаваемые для отображения различных аппаратных устройств виртуальных машин, или файлы-устройств, используемые для взаимодействия с виртуальными машинами в том числе по протоколам VNC и Spice;

– файлы процесса функционирования виртуальных машин: 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 пользователя по протоколам VNC и Spice (например, изображения рабочих столов);

– журнал регистрации событий ПК, содержащий детальную информацию по всем действиям субъектов доступа по управлению виртуальными машинами.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ЕПП — единое пространство пользователей

ОС СН — операционная система специального назначения

СЗИ — средства защиты информации

ALD — Astra Linux Directory (единое пространство пользователей)

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))

QEMU — Quick Emulator (средства эмуляции аппаратного обеспечения)

VDI — Virtual Desktop Infrastructure (инфраструктура виртуальных рабочих столов)

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					