

Утвержден
РДЦП.10001-02-УД

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

ПРОГРАММНЫЙ КОМПЛЕКС «СРЕДСТВА ВИРТУАЛИЗАЦИИ «БРЕСТ»

Руководство пользователя

РДЦП.10001-02 93 01

Листов 9

2018

Литера О₁

АННОТАЦИЯ

Настоящий документ является руководством пользователя программного комплекса «Средства виртуализации «Брест» (ПК СВ «Брест») РДЦП.10001-02 (далее по тексту — ПК).

В документе приведены общие сведения, принципы функционирования ПК, а также приведена информация о запуске виртуальной машины через консольный и графический интерфейс.

СОДЕРЖАНИЕ

1. Общие сведения	4
2. Запуск и подключение к виртуальной машине	5
2.1. Запуск и подключение к VM через консольный интерфейс	5
2.2. Запуск и подключение к VM через графический интерфейс управления виртуальными машинами	5
2.3. Удаленный доступ к VM по протоколам VNC и SPICE	6
Перечень сокращений	8

1. ОБЩИЕ СВЕДЕНИЯ

ПК предоставляет виртуальную среду, обеспечивающую функционирование виртуальных машин и управление ими в операционной системе специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (далее по тексту — ОС СН) и предназначенную для применения в автоматизированных системах в защищенном исполнении, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну, со степенью секретности до «совершенно секретно» включительно.

Пользователи ПК после прохождения процедуры идентификации и аутентификации либо выполняют запуск виртуальной машины, либо с использованием технологии VDI по протоколам VNC и SPICE получают доступ к ранее запущенным виртуальным машинам в соответствии с установленными правилами разграничения доступа. Запущенная виртуальная машина представляет собой процесс ОС СН, который функционирует от имени учетной записи пользователя с его мандатными атрибутами безопасности.

В ПК реализовано дискреционное и мандатное управление доступом к виртуальным машинам с использованием драйверов доступа в сервере виртуализации. При этом дискреционное и мандатное управление доступом к файлам-образам виртуальных машин, а также управление сетевым и межпроцессным взаимодействием между виртуальными машинами и сетевыми службами осуществляется средствами эмуляции аппаратного обеспечения совместно со средствами защиты информации ОС СН.

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

2. ЗАПУСК И ПОДКЛЮЧЕНИЕ К ВИРТУАЛЬНОЙ МАШИНЕ

Запуск виртуальной машины (VM) пользователем и подключение к ней возможны тремя способами:

- через консольный интерфейс управления виртуальными машинами (2.1);
- через графический интерфейс управления виртуальными машинами (2.2);
- через графический интерфейс для удаленного доступа (VDI) пользователя по протоколам VNC и SPICE к запущенной ранее VM (2.3).

П р и м е ч а н и е. При запуске VM приобретает динамические метки безопасности, включающие идентификатор запустившего пользователя и его мандатные атрибуты. После этого при доступе к данной виртуальной машине применяется дискреционное и мандатное управление доступом.

ВНИМАНИЕ! Только запустивший VM пользователь или пользователь, входящий в группу администраторов `libvirt-admin`, могут управлять функционированием виртуальной машины (приостанавливать, останавливать и т.п.).

2.1. Запуск и подключение к VM через консольный интерфейс

Для запуска VM через консольный интерфейс необходимо последовательно выполнить команды запуска VM и подключения к ней пользователя.

Для запуска VM используется команда:

```
virsh --connect qemu:///system start <имя_VM>
```

ВНИМАНИЕ! Для выполнения команды пользователь должен быть включен в группу `libvirt`.

Результат выполнения команды:

```
Domain <имя_VM> started
```

свидетельствует о запуске VM.

Подключение к VM выполняется с помощью команды:

```
virt-viewer --connect qemu:///system -d <имя_VM>
```

2.2. Запуск и подключение к VM через графический интерфейс управления виртуальными машинами

Для запуска VM от имени учетной записи пользователя с его мандатными атрибутами безопасности необходимо войти в ОС СН под учетной записью пользователя с заданным мандатным уровнем. Затем запустить менеджер виртуальных машин `virt-manager`, выбрать VM из списка и нажать на кнопку **[Запустить]** в соответствии с рис. 1.

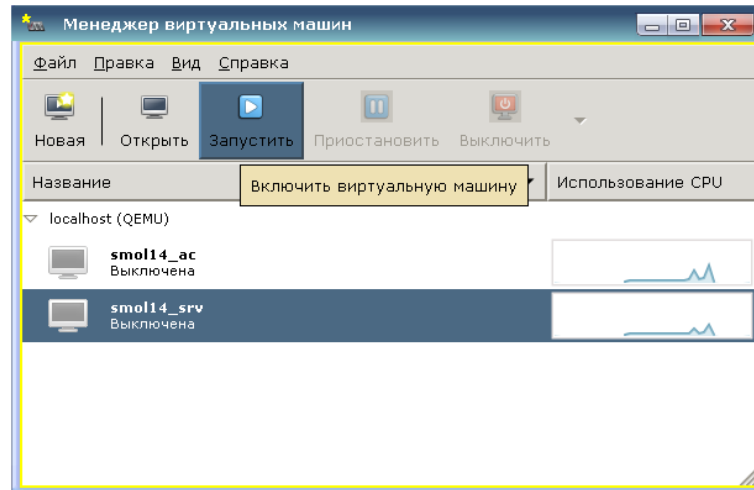


Рис. 1

2.3. Удаленный доступ к ВМ по протоколам VNC и SPICE

В состав ПК входит графический интерфейс virt-viewer, предоставляющий пользователю удаленный доступ (VDI) к рабочему столу выбранной виртуальной машины по протоколам VNC или SPICE в соответствии с рис. 2.

Для удаленного доступа к ВМ выполнить следующую команду:

1) при локальной виртуализации:

```
virt-viewer -c qemu:///system <имя_ВМ>
```

2) при серверной виртуализации:

```
virt-viewer -c qemu+tcp://<доменное_имя_пользователя>@<полное_имя_домена>  
/system <имя_ВМ>
```

ВНИМАНИЕ! Виртуальная машина должна быть уже запущена с помощью консольного или графического интерфейсов управления.

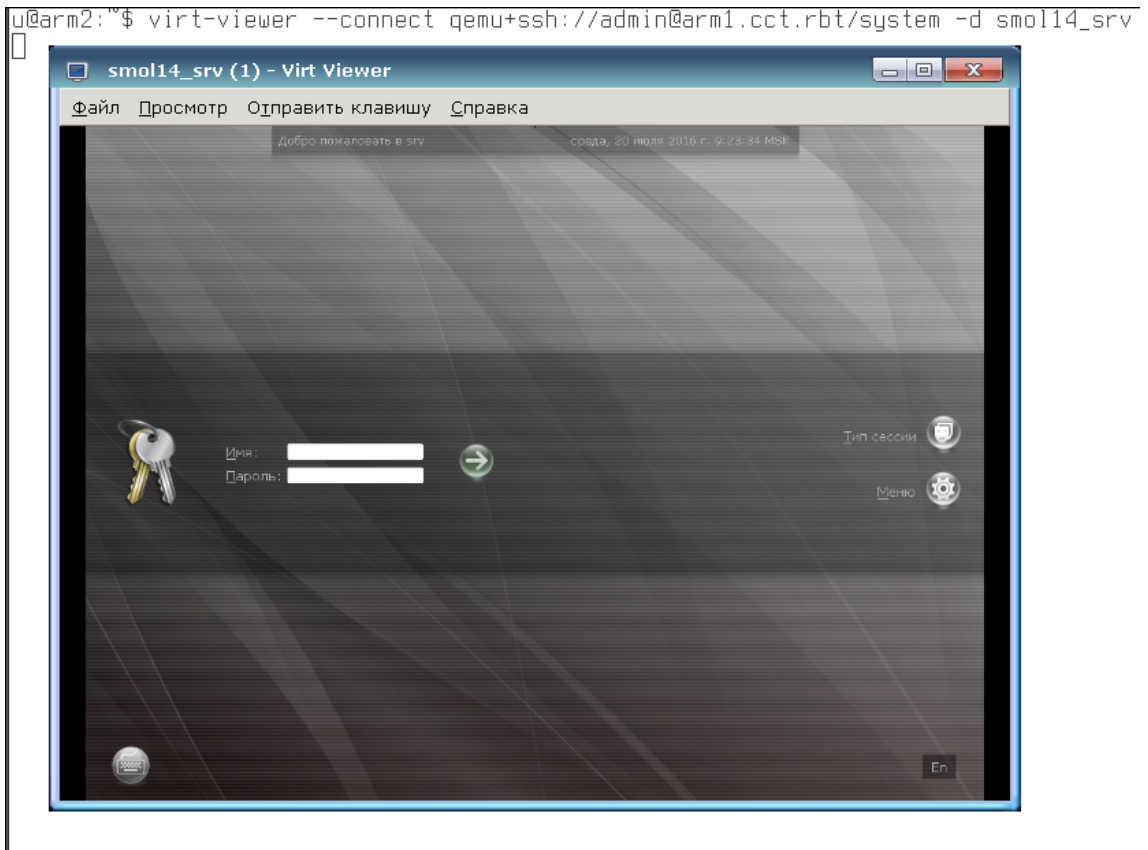


Рис. 2

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

- VM — виртуальная машина
- ОС СН — операционная система специального назначения «Astra Linux Special Edition»
- ПК — программный комплекс «Средства виртуализации «Брест»
-
- SPICE — Simple Protocol for Independent Computing Environments (простой протокол для независимой вычислительной среды)
- VDI — Virtual Desktop Infrastructure (инфраструктура виртуальных рабочих столов)
- VNC — Virtual Network Computing (система удалённого доступа к рабочему столу компьютера)

