Утвержден

РУСБ.10205-01-УД

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

ПК «ВИУ»

Руководство пользователя

РУСБ.10205-01 93 01

Листов 11

2016

АННОТАЦИЯ

Настоящий документ является руководством пользователя программного комплекса виртуализации и управления (ПК «ВИУ») РУСБ.10205-01 (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

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.

ПК обеспечивает выполнение следующих функциональных задач:

– 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.

1.1. Состав ПК

ПК состоит из компонентов, представляющих собой набор программ, сгруппированных по определенным признакам.

1) Серверная часть:
   – средства эмуляции аппаратного обеспечения;
   – сервер виртуализации;
   – служба доступа к сетевой защищенной файловой системе.
2) Клиентская часть:
   – консольный интерфейс управления виртуальными машинами;
   – графический интерфейс управления виртуальными машинами;
   – графический интерфейс для удаленного доступа (VDI) пользователей к виртуальным машинам по протоколам VNC и Spice.

Данные компоненты являются составными частями ПК, взаимодействуют между собой в процессе его функционирования и располагаются в соответствующих deb-пакетах.

1.2. Принципы функционирования

ПК функционирует под управлением ОС СН и использует архитектуру «клиент-сервер». Схема функционирования ПК в среде ОС СН представлена на рис. 1.

Серверная часть обеспечивает создание и функционирование защищенной виртуальной среды, содержащей набор виртуальных машин с определенной конфигурацией аппаратных средств и развернутыми в них гостевыми ОС.

Функционирование виртуальных машин обеспечивается модулем ядра KVM из состава ОС СН, который использует аппаратные возможности архитектуры x86-64 по виртуализации процессоров, средства эмуляции аппаратного обеспечения на основе QEMU и сервера виртуализации на основе libvirt.

Клиентские части обеспечивают удаленный доступ пользователей ПК к рабочим столам виртуальных машин с использованием технологии VDI и удаленное управление администраторами конфигурацией виртуальных машин.

С использованием консольных или графических средств осуществляется созда-

ние и настройка виртуальных машин, включая формирование конфигурации аппаратных средств виртуальных машин и установку гостевых ОС в виртуальные машины.

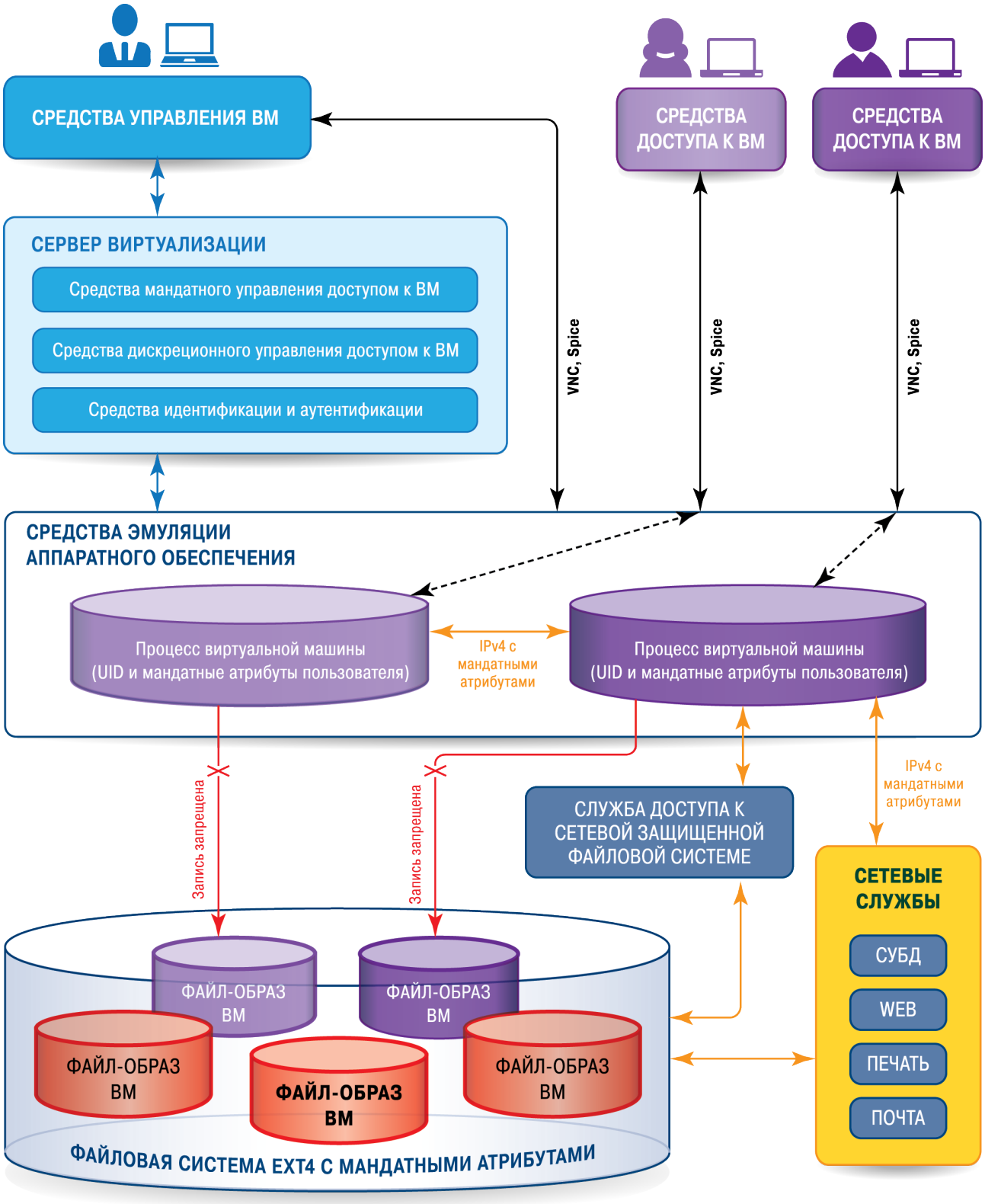

Рис. 1

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 ПК

Запуск виртуальной машины пользователем возможен 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) пользователей к виртуальным машинам по протоколам VNC и Spice (2.3).

Примечание. При запуске виртуальная машина приобретает динамические метки безопасности, включающие идентификатор запустившего пользователя и его мандатные атрибуты. После этого, при доступе к данной виртуальной машине применяются дискреционное и мандатное разграничение доступа.

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

2.1. Запуск виртуальной машины через консольный интерфейс

Для запуска виртуальной машины через консольный интерфейс необходимо выполнить команду запуска виртуальной машины и подключения к ней пользователя.

Для запуска виртуальной машины необходимо выполнить команду:

```
virsh --connect qemu:///sestem start smol14_srv
```

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

Результат вывода этой команды «`Domain smol14_srv started`» свидетельствует о запуске виртуальной машины, подключиться к которой пользователь сможет с помощью команды:

```
virt-viewer --connect qemu:///system -d smol14_srv
```

В результате выполнения команды должна запуститься виртуальная машина.

2.2. Запуск виртуальной машины через графический интерфейс управления виртуальными машинами

Для запуска виртуальной машины от имени учетной записи пользователя с его мандатными атрибутами безопасности необходимо войти в ОС СН под пользователем с заданным мандатным уровнем. После чего запустить менеджер виртуальных машин `virt-manager`, выбрать виртуальную машину из списка и нажать на кнопку «Запустить» (рис. 2).

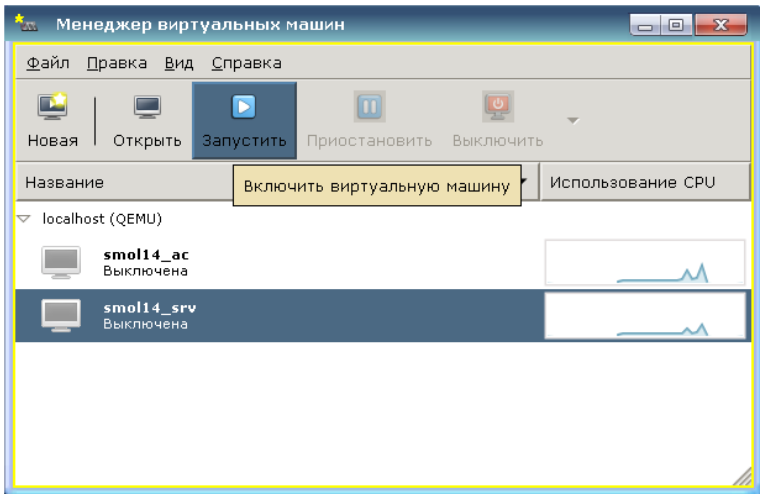

Рис. 2

2.3. Запуск виртуальной машины через графический интерфейс для удаленного доступа (VDI) пользователей к виртуальным машинам по протоколам VNC и Spice

В состав ПК входит графический интерфейс для удаленного доступа (VDI) пользователей к виртуальным машинам по протоколам VNC и Spice `virt-viewer`, предоставляющий доступ пользователя к рабочему столу выбранной виртуальной машины по протоколам VNC или Spice (см. рис. 3). Виртуальная машина должна быть уже запущена с помощью консольного или графического интерфейсов управления.

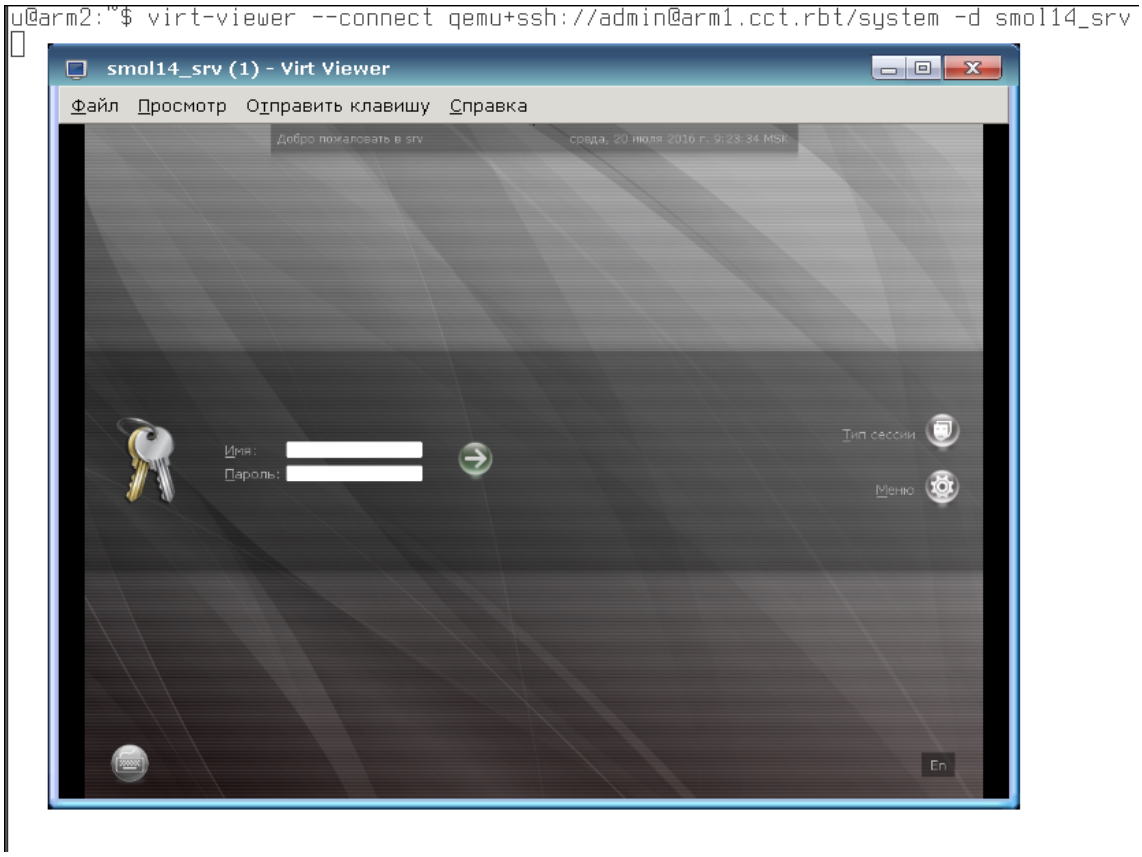

Рис. 3

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ОС СН — операционная система специального назначения

ПК — программный комплекс

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					