Утвержден

РДЦП.10001-02-УД

ПРОГРАММНЫЙ КОМПЛЕКС «СРЕДСТВА ВИРТУАЛИЗАЦИИ «БРЕСТ»

Руководство по КСЗ

РДЦП.10001-02 97 01

Листов 25

2023

Литера $О_1$

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

АННОТАЦИЯ

Настоящий документ является руководством по применению средств защиты информации «Программного комплекса «Средства виртуализации «Брест» (ПК СВ «Брест») РДЦП.10001-02 (далее по тексту — ПК СВ) и предназначен для администратора безопасности информационной системы и содержит описания:

- действий по приемке поставленного комплекта ПК СВ;
- действий по безопасной установке и настройке ПК СВ;
- действий по реализации функций безопасности среды функционирования;
- комплекса средств защиты (КСЗ).

Порядок установки и администрирования ПК СВ приведен 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». Порядок применения ПК СВ пользователями приведен в документе РДЦП.10001-02 34 01 «Программный комплекс «Средства виртуализации «Брест». Руководство пользователя».

Информация о настройке программного обеспечения, а также варианты реализации отдельных решений с использованием ПК СВ приведены на официальном информационном ресурсе: `wiki.astralinux.ru/brest`.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

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:

- 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 следующих основных положениях:

- создание среды виртуализации обеспечивается встроенными средствами ОС СН: модулем ядра KVM, который использует аппаратные возможности архитектуры x86-64 по виртуализации процессоров, средствами эмуляции аппаратного обеспечения на основе QEMU и сервером виртуализации на основе `libvirt`;

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

- ПК СВ интегрирован с комплексом средств защиты информации ОС СН;
- доверенная загрузка виртуальных машин, контроль целостности, регистрация событий безопасности, управление потоками информации, защита памяти, ограничение программной среды, идентификация и аутентификация пользователей реализуются с применением сертифицированных функций ОС СН;
- резервное копирование и управление доступом реализуется с использованием встроенных средств ПК СВ и с применением сертифицированных функций ОС СН;
- централизованное управление (администрирование) ВМ и взаимодействием между ними осуществляется встроенными средствами ПК СВ;
- в качестве службы управления единым пространством пользователей используется FreeIPA из состава ОС СН;
- функционирование защищенной среды виртуализации обеспечивается только в дискреционном режиме работы ПК СВ;
- при проектировании защищенной среды виртуализации, предназначенной для применения в автоматизированных системах, обрабатывающих информацию, ограниченного доступа, в том числе, содержащую сведения, составляющие государственную тайну, необходимо учитывать условия и ограничения, представленные в разделе 6 настоящего документа.

Администрирование ПК СВ осуществляется администратором средства виртуализации, администратором ВМ и администратором безопасности в соответствии с установленными для них полномочиями.

2. ДЕЙСТВИЯ ПО ПРИЕМКЕ ПК СВ

При приемке ПК СВ необходимо провести следующие проверки:

1) при поставке на материальном носителе:
   - проверка целостности упаковки;
   - проверка комплектности в соответствии с формуляром;
   - проверка маркировки — наличия в разделе 6 формуляра уникального идентификатора ФСТЭК России;
   - проверка контрольной суммы установочного диска;
2) при поставке по сетям связи:
   - проверка электронной подписи изготовителя образа с установочным диском ПК СВ и формуляра в формате PDF;
   - проверка комплектности в соответствии с формуляром;
   - проверка маркировки — наличия в разделе 6 формуляра уникального идентификатора ФСТЭК России;
   - проверка контрольной суммы образа установочного диска.

Порядок подсчета контрольной суммы установочного диска и (образа установочного диска) ПК СВ представлен в документе РДЦП.10001-02 30 01 «Программный комплекс «Средства виртуализации «Брест». Формуляр».

Контроль целостности программного обеспечения ПК СВ, установленного на средство вычислительной техники, подтверждаются средствами контроля целостности (средствами контроля соответствия дистрибутиву) путем вычисления и сравнения контрольных сумм исполняемых файлов и библиотек с эталонными значениями, хранящимися в файле `gostsums.txt`, размещенном на установочном диске и обновлениях ПК СВ.

3. ДЕЙСТВИЯ ПО БЕЗОПАСНОЙ УСТАНОВКЕ И НАСТРОЙКЕ ПК СВ

Действия по развертыванию и первичной настройке ПК СВ описаны в документе РДЦП.10001-02 95 01-1 «Программный комплекс «Средства виртуализации «Брест». Руководство администратора. Часть 1». При этом необходимо обеспечить выполнение следующих требований:

- контрольные суммы DVD-дисков (ISO-образа) ОС СН, рассчитанные по ГОСТ Р 34.11-2012 с использованием программы подсчета контрольных сумм `gostsum` из состава ОС СН, а также контрольные суммы DVD-дисков ОС СН, рассчитанные с использованием программы фиксации и контроля исходного состояния программного комплекса «ФИКС-UNIX 1.0» 643.53132931.501492-01 должны соответствовать значениям, приведенным в документе РУСБ.10015-01 30 02 «Операционная система специального назначения «Astra Linux Special Edition». Формуляр». Порядок подсчета контрольной суммы DVD-диска (ISO-образа) ОС СН представлен в документе РУСБ.10015-01 30 02;
- контрольные суммы CD/DVD-дисков (ISO-образа) ПК СВ, рассчитанные по ГОСТ Р 34.11-2012 с использованием программы подсчета контрольных сумм `gostsum` из состава ОС СН, должны соответствовать значениям, приведенным в документе РДЦП.10001-02 30 01. Порядок подсчета контрольной суммы DVD-диска (ISO-образа) ПК СВ представлен в документе РДЦП.10001-02 30 01.
- установку и настройку программных компонентов ПК СВ необходимо выполнять в ОС СН под учетной записью администратора с высоким уровнем целостности. При этом необходимо учитывать, что в процессе установки программных компонентов для дискреционного режима работы ПК СВ учетной записи администратора ОС СН будет присвоен максимальный уровень целостности равный 127.

После первичной настройки ПК СВ необходимо выполнить действия по реализации функций безопасности среды функционирования (см. раздел 4). Дальнейшие действия по управлению функционированием ПК СВ необходимо выполнять, основываясь на принципах ролевого управления доступом (см. 5.4).

4. ДЕЙСТВИЯ ПО РЕАЛИЗАЦИИ ФУНКЦИЙ БЕЗОПАСНОСТИ СРЕДЫ 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`.

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 и сервером виртуализации на основе `libvirt`.

Условием исключения скрытых каналов является реализуемая ОС СН политика дискреционного управления доступом, мандатного управления доступом и мандатного контроля целостности, которая является неотъемлемой частью модели политики безопасности ОС СН. Подробное описание условий исключения скрытых каналов рассмотрены в документе РУСБ.10015-01 97 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1». При этом необходимо учитывать, что функция безопасности «Мандатное управление доступом» в ОС СН доступна только на максимальном уровне защищенности («Смоленск»).

В целях обеспечения удаленного доступа пользователей с использованием сетей связи общего пользования должны применяться средства криптографической защиты информации, прошедшие процедуру оценки соответствия в соответствии с законодательством Российской Федерации.

5. ОПИСАНИЕ ФУНКЦИЙ БЕЗОПАСНОСТИ

5.1. Доверенная загрузка виртуальных машин

Доверенная загрузка виртуальных машин осуществляется с использованием следующих механизмов:

- механизм контроля конфигурации виртуального оборудования виртуальных машин;
- механизм контроля файлов виртуальной базовой системы ввода-вывода (первичного загрузчика виртуальной машины);
- механизм контроля целостности исполняемых файлов гостевой операционной системы виртуальной машины.

5.1.1. Контроль конфигурации виртуального оборудования виртуальных машин

В ПК СВ конфигурации виртуального оборудования виртуальных машин хранятся в защищенной СУБД PostgreSQL из состава ОС СН, сертифицированные функции которой обеспечивают идентификацию и аутентификацию пользователей, а также управление доступом к хранимой информации. Таким образом, при выполнении любого запроса пользователя к конфигурации ВМ осуществляется дискреционное управление доступом на основе установленных пользователю прав. Для каждой выполняемой операции производится проверка наличия права у пользователя на выполнение данной конкретной операции. Подробное описание реализации управления доступом к информации в защищенной СУБД PostgreSQL приведено в документе РУСБ.10015-01 97 01-1.

При развертывании ПК СВ дополнительная настройка целостности конфигурации виртуального оборудования не требуется.

5.1.2. Контроль файлов виртуальной базовой системы ввода-вывода

Контроль файлов виртуальной базовой системы ввода-вывода (первичного загрузчика виртуальной машины) обеспечивается механизмом контроля целостности с использованием алгоритма работы с контрольными суммами («отпечатка конфигурации»), реализованном в ОС СН. Подробное описание механизма контроля целостности «отпечаток конфигурации» приведено в документе РУСБ.10015-01 97 01-1.

Для обеспечения контроля файлов виртуальной базовой системы ввода-вывода в ПК СВ необходимо на каждом компьютере, выполняющем функцию сервера виртуализации, выполнить следующие действия:

1) установить пакеты `ovmf` и `astra-kvm-secure` командой:

```
sudo apt install ovmf astra-kvm-secure
```

2) включить механизм контроля целостности «отпечаток конфигурации». Для этого в конфигурационном файле `/etc/libvirt/libvirtd.conf` для параметра `integrity_control` установить значение «1». Конфигурирование настроек `libvirt` рекомендуется выполнять в интерактивном режиме, с использованием команды:

```
virsh -c qemu:///system config --edit-config /etc/libvirt/libvirtd.conf
```

3) перезапустить службу libvirt командой:

```
sudo systemctl restart libvirtd
```

5.1.3. Контроль целостности исполняемых файлов гостевой операционной системы

В ПК СВ используется механизм контроля целостности исполняемых файлов гостевой операционной системы, реализованный в ОС СН. Подробное описание этого механизма приведено в документе РУСБ.10015-01 97 01-1.

Для обеспечения контроля целостности исполняемых файлов гостевой операционной системы в ПК СВ необходимо на каждом компьютере, выполняющем функцию сервера виртуализации, выполнить следующие действия:

1) установить пакет `astra-kvm-secure` командой:

```
sudo apt install astra-kvm-secure
```

2) включить механизм контроля целостности исполняемых файлов гостевой операционной системы. Для этого в конфигурационном файле `/etc/libvirt/libvirtd.conf` для параметра `file_integrity_check_period_s` установить значение периода проверки в секундах, например, «60». Конфигурирование настроек `libvirt` рекомендуется выполнять в интерактивном режиме, с использованием команды:

```
virsh -c qemu:///system config --edit-config /etc/libvirt/libvirtd.conf
```

3) включить режим принудительного выключения виртуальной машины в случае нарушения целостности установленных на контроль файлов гостевой операционной системы. Для этого в конфигурационном файле `/etc/libvirt/libvirtd.conf` для параметра `file_integrity_check_shutdown_domain` установить значение «1»;

4) перезапустить службу libvirt командой:

```
sudo systemctl restart libvirtd
```

5.2. Контроль целостности

Для осуществления контроля целостности в ПК СВ используются следующие механизмы, реализованные в ОС СН:

- механизм контроля целостности «отпечаток конфигурации»;
- механизм контроля целостности исполняемых файлов гостевой операционной;

- механизм контроля запуска исполняемых файлов формата ELF и контроля расширенных атрибутов в замкнутой программной среде (ЗПС);
- механизм регламентного контроля целостности Another File Integrity Checker (AFICK);

Контроль целостности осуществляется для следующих типов объектов: конфигурации виртуального оборудования виртуальных машин, конфигураций объектов виртуальной инфраструктуры, исполняемых файлов и параметров настройки средств виртуализации, файлов виртуальной базовой системы ввода-вывода (первичного загрузчика виртуальной машины), исполняемых файлов гостевой операционной системы виртуальной машины, областей памяти виртуальной машины.

5.2.1. Настройка ПК СВ для обеспечения контроля запуска исполняемых файлов в ЗПС

Инструменты ЗПС, реализованные в ОС СН, предоставляют возможность внедрения электронной цифровой подписи (ЭЦП) в исполняемые файлы формата ELF и в расширенные атрибуты файловой системы, обеспечивая таким образом контроль целостности как в процессе загрузки средства виртуализации, так и динамически в процессе функционирования. Подробное описание инструментов ЗПС приведено в документе РУСБ.10015-01 97 01-1.

Для включения механизм контроля запуска исполняемых файлов в замкнутой программной среде необходимо на каждом компьютере, выполняющем функцию сервера виртуализации, выполнить следующие действия:

1) включить режим контроля неизменности и подлинности загружаемых исполняемых файлов командой:

```
sudo astra-digsig-control enable
```

2) перезагрузить компьютер.

5.2.2. Применение регламентного контроля целостности AFICK в ПК СВ

Организация регламентного контроля целостности объектов контроля обеспечивается программным средством AFICK из состава ОС СН путем вычисления контрольных сумм файлов и соответствующих им атрибутов расширенной подсистемы безопасности PARSEC (мандатных атрибутов и атрибутов расширенной подсистемы протоколирования) с последующим сравнением вычисленных значений с эталонными.

Программное средство AFICK (пакет `afick`) необходимо установить на каждом компьютере, выполняющем функцию сервера виртуализации. Порядок установки и настройки программного средства AFICK приведено в документе РУСБ.10015-01 97 01-1.

5.3. Регистрация событий безопасности

В ПК СВ обеспечивается регистрация событий безопасности, связанных с функционированием средств виртуализации, и оповещение администратора безопасности средства

виртуализации о событиях безопасности. Состав регистрируемой информации соответствует ГОСТ Р 59548-2022.

Регистрация событий безопасности, настройка реагирования системы на события и информирование администратора осуществляется подсистемой регистрации событий из состава ОС СН. Описание подсистемы регистрации событий и журнала событий приведено в документе РУСБ.10015-01 97 01-1. Для обеспечения регистрация событий безопасности, связанных с функционированием средств виртуализации, на каждом компьютере необходимо установить пакет `astra-kvm-secure` командой:

```
sudo apt install astra-kvm-secure
```

Для решения задач централизованного сбора журналов событий с компьютеров, на которых установлены программные компоненты ПК СВ, используется служба syslog-ng из состава ОС СН. Порядок настройки централизованного сбора журналов событий описан в документе РУСБ.10015-01 97 01-1.

5.4. Управление доступом

5.4.1. Ролевое управление доступом к виртуальным машинам

В ПК СВ реализован ролевой метод управления доступом, который подразумевает разграничение доступа по следующим ролям пользователей:

- администратор средства виртуализации;
- администратор безопасности средства виртуализации;
- разработчик виртуальной машины;
- администратор виртуальной машины.

Назначение ролей и полномочий осуществляется администратором средства виртуализации.

При развертывании службы сервера управления автоматически создается группа администраторов средства виртуализации (brestadmins). Кроме того, при инициализации службы сервера управления в ПК СВ создается первый пользователь группы администраторов средства виртуализации:

- в сервисном режиме функционирования ПК СВ — пользователь `brestadmin`;
- дискреционном режиме функционирования ПК СВ — доменный пользователь, имя которого указывается вручную при инициализации службы сервера управления.

Роль администратора средства виртуализации позволяет выполнять следующие действия:

- создавать учетные записи пользователей средства виртуализации;
- управлять учетными записями пользователей средства виртуализации;
- назначать права доступа пользователям средства виртуализации к виртуальным машинам;

- создавать и удалять виртуальное оборудование средства виртуализации;
- изменять конфигурации виртуального оборудования средства виртуализации;
- управлять доступом виртуальных машин к физическому и виртуальному оборудованию;
- управлять квотами доступа виртуальных машин к физическому и виртуальному оборудованию;
- управлять перемещением виртуальных машин;
- удалять виртуальные машины;
- запускать и останавливать виртуальные машины;
- создавать снимки состояния виртуальных машин, включающих файл конфигурации виртуальной машины, образа виртуальной машины и образа памяти виртуальной машины.

Роль администратора безопасности средства виртуализации позволяет выполнять следующие действия:

- выполнять чтение журнала событий безопасности средства виртуализации;
- формировать отчеты с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности средства виртуализации.

Роль разработчика виртуальной машины позволяет выполнять следующие действия:

- создавать виртуальные машины;
- изменять конфигурации виртуальных машин, в том числе управлять шаблонами и образами дисков виртуальных машин.

Роль администратора виртуальной машины позволяет осуществлять доступ пользователя средства виртуализации к виртуальной машине посредством интерфейса средства виртуализации.

5.4.2. Управление доступом к ресурсам виртуализации

У большинства ресурсов виртуализации ПК СВ имеются соответствующие разрешения для его владельца (owner), пользователей группы (group) и других пользователей (others). Для каждой из этих категорий можно назначить три типа полномочий: USE (применение), MANAGE (управление) и ADMIN (администрирование). Эти полномочия соответствуют следующим операциям:

- USE — операции, которые не изменяют ресурс, такие как просмотр или использование в ВМ (например, использование непостоянного образа или виртуальной сети). В основном полномочия типа USE применяются для разделения ресурсов с другими пользователями данной группы или с остальными пользователями;
- MANAGE — операции, которые изменяют ресурс, например, остановка виртуальной машины, изменение типа образа (постоянный/непостоянный) или корректировка

IP-адреса, закрепленного за ВМ. В основном полномочия типа MANAGE предоставляются пользователям, которые будут управлять ресурсами;

- ADMIN — специальные операции, предназначенные для администрирования, например, обновление данных сервера виртуализации или удаление группы пользователей.

Указанные выше полномочия могут быть применены в отношении следующих ресурсов:

- шаблоны;
- виртуальные машины;
- образы дисков;
- хранилища;
- виртуальные сети.

Кроме базовых разрешений в ПК СВ используется расширенное разрешения к ресурсам ACL (Access Control List).

Использование правил ACL позволяет администраторам адаптировать роли пользователей под нужды инфраструктуры. Например, при помощи правил ACL можно создать группу пользователей, которая будет видеть и использовать существующие виртуальные ресурсы, но не сможет создавать новые. Или можно предоставить определенному пользователю полномочия только для управления заданной группой виртуальных сетей.

Более подробно действия по управлению полномочиями, в том числе настройка правил ACL, описаны в документе РДЦП.10001-02 95 01-2 «Программный комплекс «Средства виртуализации «Брест». Руководство администратора. Часть 2».

5.4.3. Настройка ролевого управления доступом

ПК СВ Брест позволяет разделять виртуальные ресурсы на логические сущности (тенанты). Разделение осуществляется путем создания групп пользователей. Роли определяются внутри каждой группы.

Назначение ролей и полномочий необходимо выполнять в ОС СН под учетной записью администратора с высоким уровнем целостности.

Для реализации роли администратора средства виртуализации необходимо включить пользователя в следующие группы: `brestadmins`, `brestusers`, `libvirt-admins` и `admins`.

Для реализации роли администратора безопасности средства виртуализации необходимо включить пользователя в группу `astra-audit` и исключить из групп `libvirt`, `libvirt-qemu`, `kvm`. Если для просмотра журнала событий будет использоваться графическая утилита fly-event-viewer («Журнал системных событий»), то на всех компьютерах для

пользователей группы `astra-audit` необходимо разрешить привилегированный доступ к fly-event-viewer. Для этого в файле `/etc/sudoers` следует добавить следующую строку:

```
%astra-audit ALL=(ALL:ALL) /usr/bin/fly-event-viewer
```

Для реализации роли администратора ВМ необходимо включить пользователя в группу `brestusers`.

Для реализации роли разработчика ВМ необходимо выполнить следующие действия:

1) для группы, в которую входит пользователь, предоставить полномочия USE в отношении следующих ресурсов виртуализации: хранилища и виртуальные сети. Для этого создать соответствующее правило ACL командой:

```
oneacl create "@<идентификатор_группы> NET + DATASTORE /* USE"
```

2) пользователю предоставить полномочия CREATE и MANAGE в отношении шаблонов ВМ. Для этого создать соответствующее правило ACL командой:

```
oneacl create "#<идентификатор_пользователя> TEMPLATE/* CREATE+MANAGE"
```

Если пользователь совмещает роли разработчика ВМ и администратора ВМ, то необходимо выполнить следующие действия:

1) пользователю предоставить полномочия MANAGE в отношении серверов виртуализации. Для этого создать соответствующее правило ACL командой:

```
oneacl create "#<идентификатор_пользователя> HOST /* MANAGE"
```

2) пользователю предоставить полномочия CREATE в отношении остальных ресурсов виртуализации. Для этого создать соответствующее правило ACL командой:

```
oneacl create "#<идентификатор_пользователя> \
      VM+IMAGE+TEMPLATE+DOCUMENT+SECGROUP+VROUTER+VMGROUP/* CREATE"
```

5.5. Резервное копирование

В ПК СВ обеспечивается резервное копирование:

- образов виртуальных машин и конфигурации виртуального оборудования виртуальных машин;
- параметров настройки средства виртуализации;
- сведений о событиях безопасности.

Порядок действий при выполнении резервного копирования образов и конфигурации виртуального оборудования виртуальных машин представлен в документе РДЦП.10001-02 95 01-2.

Резервное копирование параметров настройки средства виртуализации реализуется с использованием следующих встроенных в ОС СН средств резервного копирования:

- комплекс программ Bacula;
- утилита копирования `rsync`;
- утилиты архивирования и копирования: `tar`, `cpio`, `gzip`, `cp`.

Описание указанных средств резервного копирования приведено в документе РУСБ.10015-01 95 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора. Часть 1». Дополнительная настройка ПК СВ не требуется.

Резервное копирование сведений о событиях безопасности реализуется с использованием встроенных в ОС СН средств ротации и архивации журналов `logrotate`, и при необходимости встроенных в ОС СН средств резервного копирования, указанных выше. Настройка ротации возможна с использованием утилиты fly-admin-events («Настройка регистрации системных событий»), которая установлена в ОС СН по умолчанию. Дополнительная настройка ПК СВ не требуется. Описание утилиты fly-admin-events приведено в электронной справке ОС СН.

5.6. Управление потоками информации

Для управления потоками информации в ПК СВ применяются следующие механизмы, обеспечивающие сетевую фильтрацию:

1) драйверы виртуальных сетей, реализованные в ПК СВ:
   - драйвер «сетевой мост с группами безопасности» (Bridged with Security Groups, далее по тексту Security Group) — устанавливаются правила iptables для внедрения правил групп безопасности;
   - драйвер VLAN — для каждой сети создается мост, к которому подключается VLAN-тегированный сетевой интерфейс (VLAN-тегирование стандарта IEEE802.1Q);
   - драйвер VXLAN — для каждой сети создается мост, к которому подключается VXLAN-тегированный сетевой интерфейс. Используемый протокол VXLAN основан на UDP-инкапсуляции и групповой адресации IP.

   При использовании перечисленных выше драйверов виртуальных сетей необходимо настроить группы безопасности, которые определяют правила сетевого фильтра в отношении трафика виртуальных машин. Порядок настройки сетевых групп безопасности представлен в документе РДЦП.10001-02 95 01-2. При этом следует учитывать, что группы безопасности не поддерживаются для адресации IPv6;
2) драйвер сетевых фильтров `libvirt`, реализованный в ОС СН, — обеспечивает полностью настраиваемую сетевую фильтрацию трафика на сетевых картах виртуальных машин с использованием сетевых фильтров `nwfilter`. Наборы правил для управления трафиком определяются на уровне сервера виртуализации. Затем наборы правил связываются с определенными сетевыми картами вирту-

альных машин. Управление сетевыми фильтрами `nwfilter` описано в документе РУСБ.10015-01 97 01-1;

3) изоляция сетей с помощью VLAN — программный многоуровневый коммутатор Open vSwitch (OVS) для виртуальных сетей из состава ОС СН обеспечивает изоляцию сети с помощью VLAN путем тегирования портов, а также фильтрацию сетевого трафика. Описание настройки и работы OVS приведено в документе РУСБ.10015-01 95 01-1.

5.7. Защита памяти

Для очистки остаточной информации в памяти средства вычислительной техники используются механизмы, реализованные в ОС СН. Указанные механизмы обеспечивают очищение неиспользуемых блоков файловой системы непосредственно при их освобождении (распределении) и очищение активных разделов страничного обмена. Описание механизмов очистки освобождаемой внешней памяти приведено в документе РУСБ.10015-01 97 01-1. Дополнительная настройка ПК СВ не требуется.

Защита задач ядра и процессов пользователей при доступе к страницам оперативной памяти обеспечивается архитектурой и параметрами ядра ОС СН. Для предупреждения несанкционированных изменений модулей ядра в составе ОС СН применяется модуль `lkrg`, который обеспечивает мониторинг угроз и блокирование несанкционированных изменений в ядре ОС СН. Таким образом, целостность всей области памяти ВМ при использовании `lkrg` обеспечивается по умолчанию. Для обработки критически важных данных рекомендуется на сервере виртуализации использовать ОС СН с включенным модулем `lkrg` и ЗПС, а в виртуальных машинах применять ОС СН на усиленном или максимальном уровне защищенности с ядром `hardened` и включенным ЗПС.

Для включения модуля `lkrg` необходимо на каждом компьютере, выполняющем функцию сервера виртуализации, выполнить следующие действия:

1) установить пакет `lkrg-<версия_ядра>`. При использовании ядра `linux-5.15-generic` команда для установки имеет следующий вид:

```
sudo apt install lkrg-5.15
```

2) перезагрузить компьютер;

3) включить использование модуля `lkrg` командой:

```
sudo astra-lkrg-control enable
```

Для изоляции и управления виртуальными гостевыми машинами используется технология KVM, которая включает специальный модуль ядра KVM и средство создания виртуального аппаратного окружения QEMU для изоляции и управления виртуальными гостевыми машинами. KVM, используя загруженный в память модуль ядра, с помощью драйвера пользовательского режима (который представляет собой модифицированный драйвер

от QEMU) эмулирует слой аппаратного обеспечения, в среде которого могут создаваться и запускаться виртуальные машины.

Более подробно механизмы защита памяти в среде виртуализации, реализованные в ОС СН, описаны в документе РУСБ.10015-01 97 01-1.

5.8. Ограничение программной среды

Контроль за запуском компонентов программного обеспечения, обеспечивающий выявление и блокировку запуска компонентов программного обеспечения, не включенных в перечень (список) компонентов, разрешенных для запуска, осуществляется следующими штатными средствами ОС СН:

1) механизмом динамического контроля целостности (режим ЗПС) исполняемых файлов и разделяемых библиотек формата ELF при запуске программы на выполнение;

2) применением режима Киоск-2, который служит для ограничения прав пользователей на запуск программ в ОС СН. Степень этих ограничений задается маской киоска, которая накладывается на права доступа к исполняемым файлам при любой попытке пользователя получить доступ.

Выявление и блокировка запуска компонентов программного обеспечения, целостность которого нарушена, осуществляется механизмом динамического контроля целостности исполняемых файлов и разделяемых библиотек формата ELF путем внедрения цифровой подписи в файлы, входящие в состав ПО. При включенном режиме контроля цифровой подписи выполняться будут только подписанные исполняемые файлы.

Порядок настройки механизма динамического контроля целостности, а также режима Киоск-2 представлен в документе РУСБ.10015-01 97 01-1.

5.9. Идентификация и аутентификация пользователей

Идентификация и аутентификация пользователей в ПК СВ выполняются с учетом требований ГОСТ Р 58833-2020 «Защита информации. Идентификация и аутентификация. Общие положения».

В сервисном режиме функционирования ПК СВ процедуры идентификации и аутентификации пользователе 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`). Порядок настройки механизма PAM представлен в документе РУСБ.10015-01 97 01-1.

В дискреционном режиме функционирования ПК СВ процедуры идентификации и аутентификации пользователей реализованы посредством службы FreeIPA из состава ОС СН. При этом аутентификация пользователей осуществляется централизованно по

протоколу Kerberos. В качестве источника данных для идентификации и аутентификации пользователей применяются службы каталогов LDAP. В этом случае необходимо, чтобы все компьютеры, на которых развернуты программные компоненты ПК СВ, входили в один домен. Порядок настройки службы FreeIPA, в том числе процедур идентификации и аутентификации пользователей, описан в документе РУСБ.10015-01 95 01-1.

5.10. Централизованное управление (администрирование) ВМ и взаимодействием между ними

Для централизованного управление образами, шаблонами (конфигурациями виртуального оборудования) и экземплярами виртуальных машин в ПК СВ используются следующие инструменты командной строки, соответственно: `oneimage`, `onetemplate`, `onevm`. Кроме того, для управления указанными функциональными элементами ПК СВ можно воспользоваться веб-интерфейсом ПК СВ. Порядок действий по централизованному управлению ВМ и взаимодействием между ними описан в документе 10001-02 95 01-2.

В ПК СВ поддерживается возможность миграции виртуальных машин с одного компьютера, выполняющего функцию сервера виртуализации, на другой. При этом миграция ВМ возможна как с остановкой, так и без остановки ее работы (при использовании общего хранилища образов). Управление перемещением виртуальных машин описано в документе 10001-02 95 01-2.

5.11. Создание кластеров высокой доступности

В ПК СВ реализована возможность объединения компьютеров, выполняющих функцию сервера виртуализации, в отказоустойчивый кластер. При выходе из строя одного сервера виртуализации виртуальные машины, размещенные на нем, будут автоматически развернуты на другом сервере виртуализации этого кластера. Распределение виртуальных машин, ожидающих запуска, между зарегистрированными серверами виртуализации осуществляет служба планировщика, реализованная в ПК СВ. Порядок управления кластером и настройка службы планировщика описаны в документе 10001-02 95 01-2.

5.12. Обновление программного обеспечения ПК СВ

В целях обеспечения соответствия требованиям безопасности информации в части устранения недекларированных возможностей и уязвимостей осуществляется ее техническая поддержка, предусматривающая выпуск очередного (планового) и оперативного (внеочередного) обновлений. Порядок выпуска и доведения обновлений до потребителей представлен в документе РДЦП.10001-02 31 01 «Программный комплекс «Средства виртуализации «Брест». Описание применения».

Обновление программного обеспечения ПК СВ выполняется с использованием следующих штатных средств ОС СН: программы установки обновлений fly-astra-update или инструмента командной строки astra-update. Порядок применения указанных средств ОС СН описывается в соответствующем бюллетене обновления безопасности.

6. ОСОБЕННОСТИ ЭКСПЛУАТАЦИИ

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.

6.1. Общие условия

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

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 ПК СВ.

Управление защищенной средой виртуализации реализуется с использованием выделенной сети управления.

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

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

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

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».

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 сервера 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.

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 сервера 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 сервера 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 сервера 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.

На одном сервере виртуализации рекомендуется настраивать ВМ одного уровня конфиденциальности.

Не рекомендуется использование гостевого агента QEMU на ненулевом уровне конфиденциальности.

При использовании ВМ с ненулевым мандатным контекстом, использование протокола ssh невозможно (ssh не работает под уровнем > 0).

Файловая система NFS в NAS не поддерживает файловые атрибуты безопасности, поэтому использование данной ФС при построении облачного хранилища недопустимо.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ВМ — виртуальная машина

ЗПС — замкнутая программная среда

КСЗ — комплекс средств защиты

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

ПК СВ — программный комплекс «Средства виртуализации «Брест»

ЭЦП — электронная цифровая подпись

NAS — Network Attached Storage (сетевое хранилище данных)

NFS — Network File System (сетевая файловая система)

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					