ООО «ВАЛИДАТА»

УТВЕРЖДЕН
ВАМБ.00060-06–ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ «ВАЛИДАТА CSP» ВЕРСИЯ 6

ФУНКЦИОНИРОВАНИЕ В ВИРТУАЛЬНОЙ СРЕДЕ

Руководство администратора информационной безопасности

ВАМБ.00060-06 93 03

2020

Аннотация

В настоящем документе приведены требования к эксплуатации в виртуальной среде средств криптографической защиты информации, в том числе ВАМБ.00060-06 «Средство криптографической защиты информации «Валидата CSP» версия 6» (далее — СКЗИ «Валидата CSP») и других программных продуктов, функционирующих совместно с СКЗИ «Валидата CSP». Далее в тексте документа ко всем средствам криптографической защиты применяется термин «СКЗИ».

Требования настоящего Руководства распространяются только на СКЗИ, обеспечивающие защиту по уровню защиты КС1. Функционирование СКЗИ, обеспечивающих защиту по уровню защиты КС2 и КС3, в виртуальной среде запрещается.

Данный документ должен применяться только вместе с документом ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности». При этом положения настоящего документа могут заменять аналогичные положения документа ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности», в этом случае требования настоящего документа являются приоритетным.

На основе настоящего Руководства и документа ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности» в эксплуатирующей организации должны быть разработаны необходимые организационные и методические документы для администраторов информационной безопасности и пользователей различных автоматизированных систем и программных комплексов с целью обеспечения эксплуатации СКЗИ в виртуальной среде.

Содержание

1 ОСНОВНЫЕ ЭЛЕМЕНТЫ ВИРТУАЛЬНОЙ СРЕДЫ

Виртуализацию можно определить как процесс представления набора вычислительных ресурсов (или их логического объединения) на основе фиксированной аппаратной базы программными средствами.

Следующие подразделы посвящены краткому описанию основных элементов виртуальной среды.

1.1 Виртуальная машина

Виртуальная машина (ВМ) — программная система, эмулирующая аппаратное обеспечение некоторой платформы и исполняющая для неё программы на так называемой хост-платформе, т.е. физической машине, на которой развёрнута виртуальная машина.

В ВМ, как и на реальный компьютер, можно устанавливать различные операционные системы (ОС) и соответствующее программное обеспечение (ПО). На одной физической машине может функционировать несколько ВМ.

1.2 Гипервизор

Гипервизор (монитор виртуальных машин) — программа или аппаратная схема, обеспечивающая или позволяющая одновременный, параллельный запуск нескольких виртуальных машин на одной физической. Гипервизор обеспечивает изоляцию ВМ друг от друга, их защиту и безопасность, разделение ресурсов между различными запущенными ОС и управление этими ресурсами. Кроме того, гипервизор может предоставлять работающим под его управлением на одном хост-компьютере ВМ средства связи и взаимодействия между собой (например, через обмен файлами или сетевые соединения) так, как если бы эти ВМ являлись различными физическими устройствами.

С программной точки зрения гипервизор представляет собой минимальную ОС, предоставляющую запущенным под его управлением ОС сервис виртуальных машин, виртуализируя (эмулируя) физическое аппаратное обеспечение конкретной машины, и управляющую этими виртуальными машинами, выделением и освобождением ресурсов для них. Гипервизор позволяет независимое включение, выключение, перезагрузку и приостановку работы любой из ВМ с той или иной ОС.

1.3 Система управления виртуальной средой

Данная система является уровнем архитектуры виртуальной среды, предназначенным для решения с помощью аппаратно-программных средств и средств сетевого взаимодействия задач управления виртуальной инфраструктурой, таких как:

– управление гипервизором (формирование настроек и задание параметров);

– настройка ВМ, виртуальных сетей, используемых хранилищ данных;

– централизация виртуальных ресурсов (обеспечение работы всех ВМ, виртуальных сетевых хранилищ данных и виртуального сетевого оборудования инфор-

мационной системы, построенной с использованием технологии виртуализации, как единой виртуальной распределённой вычислительной сети);

– управление перемещением (миграцией) ВМ с одного компьютера на другой;

– оптимизация распределенных ресурсов;

– балансировка нагрузки ВМ.

1.4 Средства защиты виртуальной среды

Имеются в виду аппаратно-программные средства, предназначенные для решения задач по защите виртуальной среды, таких как:

– контроль доступа субъектов доступа к средствам конфигурирования виртуального аппаратного обеспечения;

– резервное копирование защищаемой информации, хранимой на физических носителях информации;

– обеспечение доверенного информационного обмена (сетевого взаимодействия) внутри виртуальной инфраструктуры между администратором, пользователем и средствами защиты информации;

– идентификация и аутентификация субъектов доступа при их локальном и удалённом обращении к объектам виртуальной инфраструктуры;

– управление доступом к компонентам виртуальной среды;

– контроль целостности компонентов виртуальной среды (ПО, файлов-образов ВМ, настроек и параметров);

– защита ПО виртуальной среды от вирусного заражения;

– фильтрация сетевого трафика между компонентами виртуальной инфраструктуры и внешними сетями гипервизора.

1.5 Система хранения данных

Система хранения данных (СХД) представляет собой совокупность средств вычислительной техники, предназначенных только для хранения данных, используемых при реализации технологии виртуализации, в том числе образов ВМ и данных, обрабатываемых ВМ.

1.6 Типы гипервизоров

Ниже даётся описание основных типов гипервизоров.

1.6.1 Автономный гипервизор (Тип 1)

Гипервизоры данного типа устанавливаются на ЭВМ без предустановленной ОС, т.е. работают непосредственно на аппаратном обеспечении, контролируя как его, так и разворачиваемую виртуальную инфраструктуру. Благодаря этому гипервизоры типа 1 демонстрируют наибольшую производительность.

Примером гипервизора данного типа является гипервизор ESXi фирмы VMware, предназначенный для запуска многих ВМ на одном хостовом компьютере.

Гипервизор ESXi называют «тонким» за следующие его свойства:

– в нем отсутствует локальная сервисная консоль, являющаяся, по сути, ВМ, занимающей большую часть пространства и потребляющей большую часть ресурсов в составе гипервизора;

– установочный комплект (дистрибутив) VMware ESXi в виде ISO-образа занимает приблизительно 250 Мб. Кроме того, существует встраиваемая версия гипервизора, поставляемого со многими серверами на встроенной flash-памяти, занимающая всего 32 Mb.

1.6.2 Гипервизор на основе базовой ОС (Тип 2)

Гипервизоры типа 2 работают поверх базовой операционной системы, которая выполняется на аппаратной платформе и обеспечивает службы виртуализации, такие как поддержка устройства ввода/вывода и управление памятью. Гостевой код при этом может выполняться прямо на физическом процессоре, но доступ к устройствам ввода-вывода компьютера из гостевой ОС осуществляется через так называемый монитор уровня пользователя, являющийся обычным процессом основной ОС.

Ниже (Рисунок 1) показано, чем различаются гипервизоры типа 1 и типа 2.

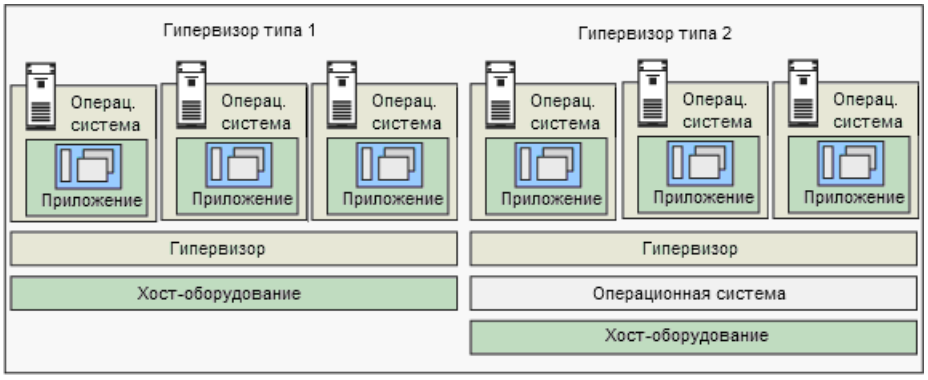

Рисунок 1 – Различия между гипервизорами типа 1 и типа 2

Примером гипервизора типа 2 является VMware Workstation.

1.6.3 Гибридный гипервизор

Гибридный гипервизор состоит из двух частей: автономного “тонкого гипервизора”, контролирующего процессор и память, а также работающей под его управлением специальной сервисной ОС. Через сервисную ОС гостевые ОС получают доступ к остальному физическому оборудованию.

Примером гибридного гипервизора является гипервизор Microsoft Hyper-V.

1.7 Виртуальная машина

Гипервизор может выделять следующие аппаратные ресурсы для ВМ:

– BIOS/UEFI;

– материнская плата;

– PCI IDE-контроллер;

– привод компакт-диска IDE;

– SCSI-контроллер;

– процессор (в зависимости от физической аппаратной части);

– сетевой адаптер;

– видеоадаптер.

Эти аппаратные ресурсы скомпонованы таким образом, чтобы обеспечить поддержку широкого круга гостевых операционных систем.

ВМ может состоять из следующих виртуальных устройств:

– процессоры: один или несколько;

– память: максимум 255 Гбайт оперативной памяти;

– SCSI-адаптеры (платы, реализующие стандарт подключения к компьютеру периферийных устройств);

– сетевые адаптеры;

– параллельные порты;

– последовательные порты;

– CD/DVD-приводы;

– USB-накопители;

– клавиатура, видеокарта и мышь.

Жёсткие диски в ВМ обычно добавляются в виде SCSI-устройств.

ВМ, по сути, представляет собой несколько файлов, хранящихся на диске хостовой ЭВМ, из которых гипервизор создаёт эмуляцию физической ЭВМ. Обычно ВМ состоит из двух файлов - файла настроек (или конфигурационного файла) и файла виртуального жёсткого диска.

1.8 Средства управления виртуальной инфраструктурой

Виртуальная инфраструктура представляет собой динамическое распределение физических ресурсов в соответствии с требованиями эксплуатирующей организации. ВМ использует материальные ресурсы одного компьютера, а виртуальная инфраструктура — материальные ресурсы всей информационно-телекоммуникационной (ИТ) среды, формируя из компьютеров, а также из подключённых к ним сетей и хранилищ единый пул ИТ-ресурсов.

Виртуальная инфраструктура включает в себя следующие компоненты:

– гипервизоры, устанавливаемые непосредственно на оборудование и обеспечивающие полную виртуализацию компьютера;

– службы виртуальной инфраструктуры, такие как управление ресурсами и консолидированное резервное копирование, которые оптимизируют использование доступных ресурсов ВМ;

– решения по автоматизации, которые предоставляют специальные средства оптимизации определенных ИТ-процессов, таких как аварийное восстановление.

Для управления инфраструктурой виртуальной среды имеются разнообразные программные средства, предназначенные для:

- управления гипервизорами;
- управления сетями;
- управления миграцией ВМ;
- управления образами и снимками ВМ, откатами и контрольными точками;
- управления системами хранения данных;
- управления развёртыванием ВМ из шаблонов;
- управления распределением нагрузки на ВМ;
- управления пулом ресурсов;
- управления конфигурациями ВМ.

Примером централизованного комплексного управления виртуальной инфраструктурой может служить System Centre Virtual Machine Manager разработки Microsoft и VMware Virtual Center разработки компании VMware.

2 ТРЕБОВАНИЯ К ЗАЩИТЕ ОТ НСД В ВИРТУАЛЬНОЙ СРЕДЕ

В настоящем разделе приведены требования к защите от несанкционированного доступа (НСД), обусловленные спецификой работы СКЗИ в виртуальной среде.

Дополнительно к требованиям настоящего документа (как для хостовой, так и для гостевой ОС) должны выполняться требования документа ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности», не противоречащие настоящему документу. В случае если требования документа ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности» противоречат требованиям настоящего документа, требования настоящего документа следует считать приоритетными.

2.1 Организация работ по защите от НСД

В организации, эксплуатирующей СКЗИ с использованием технологии виртуализации, должны быть назначены роли администраторов ВМ, осуществляющих управление компонентами (ВМ, серверными компонентами, системой хранения данных) виртуальной среды, и соответствующих администраторов информационной безопасности (АИБ) ВМ. Должны быть определены обязанности данных администраторов и разграничение их прав доступа, оптимальным образом обеспечивающие безопасность СКЗИ и виртуальной инфраструктуры в целом.

2.2 Требования к защите хостовой ЭВМ и средств виртуализации

2.2.1 Требования к техническим средствам

ЭВМ, на которых устанавливаются средства виртуализации и СКЗИ в созданной этими средствами виртуальной среде, должны быть допущены для обработки информации по действующим в РФ требованиям по защите информации от утечки по техническим каналам в соответствии с моделью угроз, принятой в эксплуатирующей организации.

Оборудование, на которое устанавливается гипервизор, не должно создавать угрозу безопасности ОС. Недопустимо использовать нестандартные аппаратные средства, имеющие возможность влиять на нормальный ход работы компьютера или ОС.

Должны быть выполнены требования по размещению физических (хостовых) ЭВМ, на которых развернуты ВМ с установленным СКЗИ, приведенные в документе ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности».

2.2.2 Требования по установке программного обеспечения на хоствую ЭВМ

К установке общесистемного и специального программного обеспечения (***в том числе программного обеспечения средств виртуализации***), а так-

же СКЗИ, допускаются лица, прошедшие соответствующую подготовку и изучившие документацию на соответствующее ПО и на СКЗИ.

При установке СКЗИ, системного и специального ПО, а также ПО средств виртуализации следует соблюдать следующие требования:

– на технических средствах, предназначенных для работы со средствами виртуализации и СКЗИ в созданной этими средствами виртуальной среде, следует использовать только лицензионное программное обеспечение фирм–производителей;

– правом установки и настройки гипервизора и гостевой ОС должен обладать Администратор ВМ, но только под контролем Администратора информационной безопасности ВМ;

– должна быть исключена возможность загрузки и использования хостовой ОС, отличной от предусмотренной штатной работой;

– должен быть организован контроль целостности ПО средств виртуализации и гипервизора в соответствии с требованиями документа ВАМБ.00060-06 93 02 «СКЗИ «Валидата CSP» версия 6. Контроль целостности. Руководство администратора информационной безопасности».

2.2.3 Настройка хостовой ЭВМ

Администратор информационной безопасности ВМ должен сконфигурировать хостовую ЭВМ и средства виртуализации, в среде которой планируется использовать СКЗИ, и осуществлять периодический контроль выполненных настроек в соответствии со следующими требованиями:

– в BIOS/UEFI хостовой ЭВМ должны быть заданы установки, исключающие возможность загрузки хостовой ОС, отличной от установленной на жестком диске: отключается возможность загрузки с гибкого диска, привода CD-R и прочие нестандартные виды загрузки ОС, включая сетевую загрузку. Не применяются ЭВМ с BIOS/UEFI, исключающими возможность отключения сетевой загрузки ОС;

– должна быть исключена возможность удалённого управления, администрирования и модификации хостовой ОС и её настроек;

– серверы виртуализации с установленными на них ВМ с СКЗИ не должны быть подключены к сетям, доступ к которым не ограничен определённым кругом лиц.

– средствами BIOS/UEFI хостовой ЭВМ должна быть исключена возможность отключения пользователями ISA и PCI устройств при использовании СЗИ от НСД, устанавливаемых в ISA и PCI разъем;

– необходимо предусмотреть меры, исключающие возможность несанкционированного необнаруживаемого изменения аппаратной части хостовой ЭВМ (например, путем опечатывания системного блока и разъемов хостовой ЭВМ);

– для гипервизора необходимо использовать статический IP-адрес;

– необходимо отключить SDK гипервизора (Managed Object Browser);

– необходимо установить на максимальный уровень безопасности использование VIB пакетов (VMWare Certified);

– для управления гипервизором, для взаимодействия гипервизора с СХД и для взаимодействия гипервизора с ВМ должны использоваться как минимум три различных виртуальных коммутатора (VSwitch).

2.2.4 Эксплуатация хостовой ЭВМ и средств виртуализации

При эксплуатации СКЗИ в виртуальной среде должны соблюдаться следующие требования:

– должна быть исключена возможность работы на хостовой ЭВМ с установленной ВМ, на которой эксплуатируется СКЗИ, если во время её начальной загрузки не проходят встроенные тесты, а также если имеются сбои или отказы в работе программно-аппаратных СЗИ от НСД;

– периодически Администратором информационной безопасности должны контролироваться сохранность оборудования и целостность печатей на хостовой ЭВМ;

– запрещается снятие задач с выполнения при помощи выключения питания хостовой ЭВМ или нажатия на кнопку «RESET» на системном блоке (для выхода из работы необходимо применять штатные процедуры, принятые в соответствующей ОС);

– запрещается несанкционированное вскрытие системных блоков и работа при нарушении целостности печатей (на системных блоках);

– запрещается вносить какие-либо изменения в программное обеспечение средств виртуализации, ВМ и СКЗИ.

2.2.5 Система управления виртуальной средой

Система управления виртуальной средой должна располагаться в одной контролируемой зоне (КЗ) с серверными компонентами виртуальной среды.

При организации удалённого управления ВМ в пределах КЗ для данного управления должен использоваться выделенный сегмент локальной сети, не имеющий выхода во внешние сети.

Примечание — Виртуальная инфраструктура (инфраструктура виртуализации, виртуальная среда) — в зависимости от контекста либо множество программно-аппаратных средств, обеспечивающих развёртывание ВМ, либо сами эти ВМ и система их связей между собой.

При необходимости использования для удалённого управления ВМ каналов связи, проходящих через пространство вне КЗ, данные каналы должны быть защищены средствами шифрования, имеющими сертификат уполномоченного органа. Для согласования сеансовых ключей шифрования необходимо использовать криптографические протоколы (такие, как Kerberos, TLS, протоколы IPSec), обеспечивающие защиту сеансовых ключей и аутентификацию взаимодействующих сторон.

При этом рабочее место администратора ВМ должно находиться в пределах предназначенной для него КЗ.

Сеть управления виртуальной средой должна быть выделена в отдельный сетевой сегмент. Для защиты данного сегмента должны использоваться средства межсетевого экранирования и предотвращения вторжений.

Сеть управления виртуальной инфраструктурой не должна подключаться к

общедоступным сетям (сетям, доступ к которым не ограничен определённым кругом лиц).

2.2.6 Требования к системе хранения данных

В СХД должны быть выделены логические разделы, предназначенные для хранения:

– эталонных образов ВМ с установленными на них СКЗИ;

– параметров настройки гипервизора и программного обеспечения, необходимого для его функционирования.

Доступ к СХД должен осуществляться только с использованием средства виртуализации (гипервизора) и системы резервного копирования. Прямой доступ к СХД с рабочих мест пользователей не допускается.

Доступ к логическим разделам СХД, используемым для хранения эталонных образов ВМ с установленными на них СКЗИ и для хранения данных гипервизора и программного обеспечения, необходимого для его функционирования, должен предоставляться только для рабочих мест администраторов ВМ.

Средства вычислительной техники (СВТ) и программное обеспечение, используемое для функционирования и управления СХД, а также рабочие места, используемые для целей управления и администрирования СХД, должны находиться в пределах КЗ.

Рабочие места, используемые для выполнения задач управления и администрирования СХД, должны располагаться в специально выделенном сегменте локальной вычислительной сети. Размещение в указанных сетевых сегментах СВТ, не связанных с выполнением задач администрирования СХД, не допускается. Выполнение задач, связанных с управлением и администрированием СХД, с использованием иных рабочих мест должно быть запрещено сертифицированными сетевыми техническими средствами.

Должен выполняться контроль целостности программного обеспечения СХД, в том числе, при загрузке указанного программного обеспечения.

Для доступа к логическим разделам СХД с образами ВМ с установленными на них СКЗИ должен использоваться символьный пароль, соответствующий требованиям документа ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности».

Сегмент локальной сети, выделенный для обеспечения доступа к управляющим интерфейсам СХД, должен быть изолирован от сетей общего пользования.

Должно быть обеспечено разграничение доступа к файлам образов дисков ВМ, хранящихся в СХД.

2.2.7 Требования к миграции образов ВМ

Миграция образов ВМ с установленным на них СКЗИ должна осуществляться в выделенном изолированном сегменте локальной сети в пределах контролируемой зоны.

При передаче образов ВМ через пространство вне КЗ необходимо использовать каналы, защищённые средствами шифрования, имеющими сертификат уполномоченного органа. При этом для согласования сеансовых ключей шифрования необходимо использовать криптографические протоколы (такие, как

Kerberos, TLS, протоколы IPSec), обеспечивающие защиту сеансовых ключей и аутентификацию взаимодействующих сторон.

2.2.8 Защита от сетевых атак на гипервизор

Доступ к интерфейсам гипервизора и средств управления виртуальной инфраструктурой с плацдарма, находящегося вне КЗ, должен осуществляться с использованием криптографических протоколов, обеспечивающих аутентификацию взаимодействующих сторон, контроль целостности и, при необходимости, шифрование передаваемой информации.

Должны быть реализованы следующие меры:

– использование межсетевых экранов и систем предотвращения вторжений для фильтрации сетевого трафика системы управления ВМ и блокирования сетевых атак;

– своевременная установка обновлений безопасности ПО гипервизора;

– отделение продуктивной сети от сети управления серверами виртуализации;

– контроль целостности ПО и настроек гипервизора;

– регистрация действий администраторов виртуальной среды.

2.2.9 Защита от атак, использующих неполную изоляцию ВМ

Настройками гипервизора должно быть обеспечено выполнение следующих требований:

– выделение для каждой ВМ отдельной области оперативной памяти хостовой машины;

– запрет информационного обмена между ВМ с использованием общих ресурсов хостовой машины, в том числе общих областей оперативной памяти хостовой машины;

– запрет информационного обмена между ВМ и программными процессами и операционной системой хостовой машины, на которой функционирует гипервизор, с использованием общих ресурсов хостовой машины, в том числе общих областей оперативной памяти хостовой машины;

– запрет информационного обмена между программными процессами, используемыми для доступа пользователей к ВМ, и иными программными процессами с использованием общих (разделяемых) ресурсов.

2.2.10 Требование к управлению доступом

Штатными средствами виртуализации должно выполняться управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри ВМ.

2.2.11 Требование к регистрации событий

Штатными средствами виртуализации должна выполняться регистрация событий безопасности в виртуальной инфраструктуре.

2.3 Требования к защите ВМ

2.3.1 Настройка гостевой ОС

Администратор информационной безопасности ВМ должен сконфигурировать гостевую ОС, в среде которой планируется использовать СКЗИ, и осуществлять периодический контроль выполненных настроек в соответствии со следующими требованиями (дополнительными по отношению к перечисленными в документе ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности»):

– необходимо исключить одновременную работу в ОС с работающим СКЗИ и загруженной ключевой информацией нескольких пользователей в случае, когда невозможно организационно-техническими мерами исключить доступ пользователя к ключевой информации других пользователей;

– ВМ с установленными на них СКЗИ не должны быть подключены к сетям, доступ к которым не ограничен определённым кругом лиц;

– запрещается использование VMWare Tools;

– запрещается использование приостановки ВМ (режим Suspend);

– при использовании VCenter рекомендуется отключить прямой доступ к гипервизору (Enable Lockdown Mode).

2.3.2 Требования к созданию снапшотов

Должно быть запрещено создание снапшотов при работающем СКЗИ.

2.3.3 Защита удалённой загрузки ключей

Должна быть обеспечена защита ключевой информации средствами шифрования, имеющими сертификат уполномоченного органа. При этом рабочее место АИБ ВМ, осуществляющего удалённую загрузку ключей, должно находиться в пределах отведённой для него контролируемой зоны.

Для удалённой загрузки ключей в ВМ (или в терминальную сессию на виртуальном сервере) пользователь на своей рабочей станции с ОС Windows и с установленным СКЗИ должен использовать ключевой носитель типа смарт-карта, например, vdToken. Пользователь подключается к своей ВМ или терминальной сессии по протоколу TLS или IPSec (который оборачивает и защищает протокол RDP). При этом его ключевой носитель становится доступным в ВМ или терминальной сессии для загрузки (если ключ извлекаемый) или для вычисления ЭП и шифрования (если ключ не извлекаемый), т.к. ВМ (терминальная сессия) «видит» vdToken пользователя по протоколу PC/SC.

В данном случае как загрузка ключа, так и обмен данными между удалённой рабочей станцией и рабочим местом АИБ ВМ должны быть защищены сертифицированной реализацией протокола TLS (или IPSec).

Для согласования сеансовых ключей шифрования, используемых для защиты каналов удалённой загрузки, необходимо использовать криптографические протоколы (такие, как Kerberos, TLS, протоколы IPSec), обеспечивающие защиту сеансовых ключей и аутентификацию взаимодействующих сторон.

2.3.4 Защита от сетевых атак между ВМ

ВМ с установленными на них СКЗИ должны размещаться в отдельных сегментах локальных сетей в пределах КЗ.

Разделение указанных сегментов локальных сетей и информационный обмен между ними должны осуществляться только с использованием физических сетевых технических средств.

Должен быть запрещен информационный обмен между ВМ с использованием общих ресурсов хостовой машины, в том числе общих областей оперативной памяти хостовой машины.

Для оперативной памяти выполнение данного требования автоматически обеспечивается средствами Hyper-V и VMWare. Необходимо также обеспечить невозможность подключения по сети ВМ к своей хостовой машине (настройками брандмауэра и/или сетевыми политиками) и невозможность чтения дисков хостовой машины в ВМ (настройками ВМ, касающихся доступа к локальным ресурсам).

2.3.5 Требования к аутентификации администратора гипервизора

Для аутентификации администратора гипервизора должен использоваться символьный пароль соответствующий требованиям, приведенным в документе ВАМБ.00060-06 93 01 «СКЗИ «Валидата CSP» версия 6. Руководство администратора информационной безопасности».

3 КОНТРОЛЬ ЦЕЛОСТНОСТИ ПО

Необходимо организовать ПО СКЗИ и гостевой ОС в соответствии с требованиями документа ВАМБ.00060-06 93 02 «СКЗИ «Валидата CSP» версия 6. Контроль целостности. Руководство администратора информационной безопасности». Перечень файлов, подлежащих контролю целостности приведён в эксплуатационной документации СКЗИ.

3.1 Контроль целостности ПО виртуальной среды

Необходимо выполнять контроль целостности следующих компонентов виртуальной среды:

– ПО гипервизора (сервера виртуализации);

– настроек гипервизора;

– образов ВМ, в том числе, эталонных образов ВМ, использующихся при развёртывании новых ВМ;

– ПО серверов управления виртуальной инфраструктурой.

Для контроля целостности программных компонентов виртуальной среды функционирования СКЗИ следует использовать программные и/или аппаратные средства защиты от НСД, сертифицированные ФСБ России.

Рекомендуется использовать регламент контроля целостности программных компонентов виртуальной среды, аналогичный регламенту контроля целостности ПО среды функционирования СКЗИ на аппаратной (физической) платформе (см. документ ВАМБ.00060-06 93 02 «СКЗИ «Валидата CSP» версия 6. Контроль целостности. Руководство администратора информационной безопасности»).

Примечание – Возможен вариант контроля целостности файлов внутри ВМ из хостовой ОС при использовании ПО, позволяющего «видеть» файлы на диске ВМ из хостовой ОС.

3.2 Требования к эталонным и загрузочным образам ВМ

При создании эталонных образов ВМ предварительно должна быть выполнена проверка:

– соответствия параметров и настроек ВМ установленным требованиям безопасности;

– целостности системного ПО гостевой ОС и ПО СКЗИ с использованием сертифицированных средств контроля целостности (см. документ ВАМБ.00060-06 93 02 «СКЗИ «Валидата CSP» версия 6. Контроль целостности. Руководство администратора информационной безопасности»).

После создания эталонного образа (клона) ВМ должна быть выполнена контрольная установка ВМ с данного образа и контрольная проверка целостности системного ПО гостевой ОС и ПО СКЗИ.

В случае успешной проверки с использованием программы контроля целостности (HASHFILE.EXE) должен быть выполнен расчёт контрольного значения файла-образа для последующей проверки целостности эталонного образа.

Перед установкой эталонного образа на сервере виртуализации (гипервизоре) должна быть выполнена проверка его целостности.

Для каждого эталонного образа ВМ должны выполняться процедуры обновления настроек, включённых в образ программных компонент СКЗИ.

Должно выполняться своевременное обновление настроек ВМ, включённых в эталонный образ.

Должна выполняться своевременная установка обновлений безопасности ОС, включённой в эталонный образ.

Загрузочные образы должны создаваться только для ВМ, созданных с использованием эталонных образов. При этом должно быть исключено внесение в эталонный образ изменений, выполненных при создании загрузочных образов.

Должно быть запрещено копирование текущих образов ВМ, включающих в себя СКЗИ.

Должен быть регламентирован поэкземплярный учёт используемых эталонных образов ВМ, а также поэкземплярный учёт СКЗИ, устанавливаемых с использованием загрузочных образов.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АРМ	Автоматизированное рабочее место
ВМ	Виртуальная машина
ИТ	Информационно-телекоммуникационный (среда, ресурсы и т.д.)
КЗ	Контролируемая зона
ОС	Операционная система
ПК	Программный комплекс
ПО	Программное обеспечение
СВТ	Средства вычислительной техники
СКЗИ	Средство криптографической защиты информации
СФК	Среда функционирования криптосервера
СХД	Система хранения данных
ЭВМ	Электронная вычислительная машина

Лист регистрации изменений

Номера листов (страниц)					Всего листов (страниц) в докум	№ документа	Входящий № сопроводительного докум и дата	Подп	Дата
Изм	изменённых	заменённых	новых	аннулированных					