127018, Москва, Сущёвский Вал, 18
Телефон: (495) 995 4820
https://CryptoPro.ru
E-mail: info@CryptoPro.ru

Средство
Криптографической
Защиты
Информации

КриптоПро CSP
Версия 5.0 R3 КС1
(исполнение 1-Base)
Руководство администратора
безопасности.
Использование СКЗИ
в виртуальных средах.

ЖТЯИ.00101-03 91 09
Листов 14

2024 г

Содержание

Аннотация

Настоящее руководство содержит требования и рекомендации по использованию СКЗИ в виртуальных средах.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ «КриптоПро CSP» версия 5.0 R3 KC1 (исполнение 1-Base) в виртуальных средах, должны разрабатываться с учетом требований настоящего документа.

Перечень определений и сокращений

Виртуализация (эмуляция)	Процесс копирования функций одной вычислительной системы на другую с использованием специально предназначенного для этого комплекса программных и/или аппаратных мер так, чтобы копируемые функции как можно ближе соответствовали поведению оригинала; как правило, под виртуализацией на практике называют полную эмуляцию аппаратной платформы или паравиртуализацию.
Полная виртуализация аппаратной платформы	Эмуляция этой платформы, предоставляющая для запускаемых на ней программ интерфейсы, идентичные интерфейсам эмулируемой платформы; запускаемое на данной виртуальной платформе программное обеспечение (начиная с ОС) не требует модификаций.
Паравиртуализация	Эмуляция платформы, предоставляющая для запускаемых на ней программ интерфейсы, схожие с интерфейсами эмулируемой платформы, но не идентичные им; запускаемое на данной виртуальной платформе программное обеспечение (начиная с ОС) должно быть модифицировано/доработано.
Виртуализация уровня операционной системы («контейнеризация»)	Эмуляция программного компонента среды функционирования с возможностью более строгого её определения и ограничения; эмуляция реализуется на базе ядра операционной системы (потому имеет ограничения в выборе эмулируемой операционной системы) и на основе механизмов разграничения доступа к аппаратным и программным ресурсам.
Виртуальная машина (ВМ)	Результат эмуляции (полной или частичной) аппаратной платформы.
Гипервизор (монитор виртуальных машин)	Программное и/или аппаратное средство, обеспечивающее: • одновременную, параллельную работу на одной физической машине нескольких виртуальных машин; • изоляцию ресурсов виртуальных машин друг от друга; • распределение ресурсов физической машины по виртуальным.
Снапшот	Копия данных виртуальной машины и всего состояния системы в определенный момент времени.
Демон (серверная часть) средств контейнеризации *(актуально для технологии Docker)*	Аналог гипервизора для контейнеров, обеспечивающий выполнение функций создания, запуска, контроля работы контейнеров, изоляции их ресурсов друг от друга и распределения ресурсов физической машины.
Клиент средств контейнеризации *(актуально для технологии Docker)*	Программные средства, предоставляющие интерфейс для взаимодействия с Демоном средств контейнеризации и отправки ему команд на исполнение.
Образ	Неизменяемый шаблон, из которого разворачивается рабочая копия эмуляции программного компонента СФ с работающим в этой СФ ПО. Образы состоят из нескольких слоёв, каждый из которых представляет собой защищенную от записи файловую систему. В общем случае образ может содержать не полноценную ОС, а только необходимый набор её модулей.

Контейнер	Исполняемый экземпляр, развернутый из образа. Разворачивание контейнера сопровождается добавлением поверх образа новых слоёв для чтения и записи. Из одного образа можно создать и запустить несколько контейнеров.
«Движок», или Средство контейнеризации	Набор программных средств, обеспечивающих выполнение функций создания, запуска, контроля работы контейнеров, изоляции их ресурсов друг от друга и распределения выделяемых контейнерам ресурсов физической машины.
Оркестратор контейнеров	Набор инструментов для управления инфраструктурой контейнеров: автоматизации развёртывания контейнеров, управления ими, масштабирования, управления сетью, координации обновления приложений, мониторинга и т.д.
Гостевая (эмулируемая) ОС	ОС, установленная на виртуальной машине/в контейнере.
Хостовая (основная) ОС	ОС, установленная на физической ПЭВМ, в среде которой функционирует гипервизор/средство контейнеризации.
Виртуальная инфраструктура (инфраструктура виртуализации, виртуальная среда)	Множество программно-аппаратных средств, обеспечивающих развёртывание виртуальных машин/контейнеров, либо сами виртуальные машины/ контейнеры и система их связей между собой.
Система управления виртуальной средой	Набор инструментов для управления инфраструктурой виртуальных машин, обеспечивающий: • управление гипервизором (формирование настроек и задание параметров); • настройку виртуальных машин, виртуальных сетей, используемых хранилищ данных; • централизацию виртуальных ресурсов (обеспечение работы всех виртуальных машин, виртуальных сетевых хранилищ данных и виртуального сетевого оборудования информационной системы, построенной с использованием технологии виртуализации, как единой виртуальной распределённой вычислительной сети); • управление перемещением (миграцией) виртуальных машин с одного компьютера на другой.

1 Поддерживаемые виртуальные среды

СКЗИ «КриптоПро CSP» версия 5.0 R3 КС1 (исполнение 1-Base) используется в следующих виртуальных средах:

Программно-аппаратные виртуальные среды:

Microsoft Hyper-V Server 2008/2008R2/2012/2012R2/2016/2019 (x64)
Microsoft Hyper-V 8/8.1/10 (x64)
Citrix XenServer 7 (x64)
Citrix Hypervisor 8.0/8.1/8.2 (x64)
VMWare WorkStation 11/12/14/15/16 (x86, x64)
VMWare WorkStation Player 12/14/15 (x86, x64)
VMWare vSphere ESXi/Hypervisor 5.5/6.0/6.5/6.7/7.0 (x64)
Oracle VirtualBox 5.2/6.0/6.1/7.0 (x86, x64)
RHEV 4 (x64)
ROSA Virtualization (x64)
Альт Сервер Виртуализации 9 (x64, ARM64)
ПК «Средства виртуализации «БРЕСТ» в составе ОС «Astra Linux Special Edition»
KVM из состава поддерживаемых ОС (x64), в т.ч. совместно с Libvirt 6/7/8 (x64)
QEMU 4.2/5.2/6.2/7 (x64)
Yandex KVM YC 5.10 (x64)
Yandex QEMU YC 5.0.1 (x64)
Proxmox VE 7 (x64) в режиме администрирования ВМ

Программные виртуальные среды (средства контейнеризации):

Docker Engine 20.10 (x64, ARM)
Kubernetes 1.24, 1.25 (x64)
OpenShift Container Platform 4.10, 4.11 (x64)

В качестве гостевых ОС допускается использовать программно-аппаратные платформы, перечисленные в п. 3.2 ЖТЯИ.00101-03 30 01. Формуляр.

2 Требования по обеспечению безопасности при эксплуатации СКЗИ в виртуальных средах

2.1 Ролевая модель

Необходимо наличие как минимум двух функциональных ролей виртуальной инфраструктуры:

1) Администратор виртуальной среды, осуществляющий управление и настройку компонентов виртуальной инфраструктуры: ресурсов виртуальных машин/контейнеров, гепервизоров/демонов средств контейнеризации, систем управления виртуальной средой/оркестраторов, серверных компонентов, систем хранения данных.

2) Администратор безопасности, осуществляющий администрирование виртуальных машин/ контейнеров.

Допускается объединение указанных ролей с учётом модели угроз и нарушителя информационной системы, в которой применяется СКЗИ, а также с учетом нормативных документов, определяющих создание такой информационной системы.

2.2 Установка ПО

Инсталляция СКЗИ на рабочих местах должна производиться только с дистрибутива, полученного по доверенному каналу (раздел 2 документа ЖТЯИ.00101-03 95 01. Правила пользования).

К установке общесистемного и специального программного обеспечения, а также СКЗИ, допускаются лица, прошедшие соответствующую подготовку и изучившие документацию на соответствующее ПО и СКЗИ.

Требования к установке программного обеспечения и СКЗИ в гостевой и хостовой ОС:

• На технических средствах, предназначенных для работы со средствами виртуализации, и в созданной этими средствами виртуальной среде следует использовать только лицензионное ПО.

• При установке ПО виртуализации, гостевой ОС и СКЗИ необходимо провести контроль целостности соответствующего дистрибутива. Дистрибутив при этом должен быть получен доверенным образом (см. раздел 2 документа ЖТЯИ.00101-03 95 01. Правила пользования).

• На ПЭВМ и в виртуальной среде не должны устанавливаться средства разработки ПО и отладчики. Если средства отладки приложений нужны для технологических потребностей организации, то их использование должно быть санкционировано администратором безопасности. При этом должны быть реализованы меры, исключающие возможность использования этих средств для редактирования кода и памяти СКЗИ и приложений, использующих СКЗИ, а также для просмотра кода и памяти СКЗИ и приложений, использующих СКЗИ, в процессе обработки СКЗИ защищаемой информации и/или при загруженной ключевой информации.

• После завершения процесса установки должны быть выполнены действия, необходимые для осуществления периодического контроля целостности установленного ПО СКЗИ и его окружения в соответствии с документацией (см. ЖТЯИ.00101-03 95 01. Правила пользования).

• После завершения процесса создания ВМ/контейнера, выполнения требуемых настроек и задания требуемых параметров, должны быть выполнены действия, необходимые для осуществления периодического контроля целостности настроек и параметров ВМ/контейнера (см. ЖТЯИ.00101-03 95 01. Правила пользования).

В табл. 1 приведены сведения о расположении конфигурационных файлов поддерживаемых виртуальных сред.

Таблица 1. Расположение конфигурационных файлов виртуальных сред

Виртуальная среда	Расположение конфигурационных файлов
Microsoft Hyper-V	конфигурационный файл по умолчанию располагается в папке `C:\ProgramData\Microsoft\Windows\Hyper-V`, имя файла совпадает с именем ВМ
Citrix	информация о конфигурации ВМ хранится в специализированной базе метаданных, дублированной на всех хостах (гипервизоре); администратор, обладающий необходимыми правами, может осуществить экспорт ВМ вместе с метаданными в одном из стандартных форматов (VHD или OVF), а также осуществить резервное копирование метаданных ВМ
VMWare	конфигурационный файл находится в той же директории, что и образ ВМ, имеет расширение .vmx и название, совпадающее с именем ВМ
Oracle Virtual Box	конфигурационный файл находится в той же директории, что и образ ВМ, имеет расширение .vbox и название, совпадающее с именем ВМ
RHEV	конфигурационный файл по умолчанию располагается в директории `/etc/libvirt`, имя файла совпадает с именем ВМ
ROSA Virtualization	конфигурационные файлы имеют расширение .conf и располагаются в директориях `/var/lib/ovirt-hosted-engine- setup` и `/etc/ovirt-hosted-engine`
Альт Сервер Виртуализации	файлы конфигурации ВМ хранятся в файловой системе кластера PVE и доступны в каталоге `/etc/pve/qemu-server/<VMID>.conf`
KVM, QEMU, Средства виртуализации «БРЕСТ»	информация о конфигурации ВМ хранится в XML-файлах с расширением .conf, конфигурационные файлы хранятся в директории `/etc/libvirt`
Docker	конфигурационный файл расположен в `%USERPROFILE%\.docker` для Windows, `/etc/docker` для Linux и `~/.docker` для Mac OS
Kubernetes	конфигурационный файл расположен в `%USERPROFILE%\.kube\config` для Windows, `~/.kube/config` для Linux/Unix
OpenShift	конфигурационные файлы .yaml расположены в `/etc/origin/master` и `/etc/origin/node`

• После завершения процесса установки гостевой ОС должны быть выполнены действия, необходимые для осуществления периодического контроля целостности установленного в гостевой ОС системного ПО в соответствии с приведённым в документации СКЗИ списком файлов, подлежащих контролю целостности.

• Предусмотреть меры, исключающие возможность несанкционированного не обнаруживаемого изменения аппаратной части технических средств, на которых установлены СКЗИ и компоненты виртуальной инфраструктуры (например, путем опечатывания системного блока и разъемов ПЭВМ).

Примечание. При использовании средств контейнеризации запуск проверки целостности ПО и СКЗИ в контейнере и поиска поврежденных (corrupted) библиотек СКЗИ рекомендуется выполнять из хостовой ОС для обеспечения возможности завершения работы контейнера в случае обнаружения нарушений целостности.

2.3 Настройка гипервизора/демона средств контейнеризации

Настройками гипервизора/демона средств контейнеризации должно быть обеспечено выполнение следующих требований:

• Для каждой ВМ/контейнера должна быть выделена отдельная область оперативной памяти хостовой машины.

• Необходимо обеспечить невозможность информационного обмена между ВМ/контейнерами с использованием общих ресурсов хостовой машины. При этом допускается информационный обмен между ВМ/контейнерами с использованием ресурсов гостевых ОС.

• Необходимо обеспечить невозможность информационного обмена между ВМ/контейнерами, программными процессами и ОС хостовой машины, на которой функционирует виртуальная инфраструктура, использованием общих ресурсов хостовой машины.

• Необходимо обеспечить невозможность информационного обмена между программными процессами, используемыми для доступа пользователей к ВМ/контейнерам, и иными программными процессами с использованием общих, разделяемых ресурсов.

2.4 Требования по защите от НСД при эксплуатации СКЗИ

Запрещено:

• оставлять без контроля вычислительные средства, на которых эксплуатируется ВМ/контейнер с установленным СКЗИ, и клиентские места (терминалы) после ввода ключевой информации либо иной конфиденциальной информации;

• оставлять без контроля клиентские места (терминалы) пользователей виртуальных рабочих столов с установленными на них СКЗИ;

• вносить какие-либо изменения в ПО виртуализации и СКЗИ;

• включать в образ контейнера приложение на базе СКЗИ, если:

– ДСЧ в составе СКЗИ находится в инициализированном состоянии;

– в образ включена внешняя гамма, используемая в качестве исходного материала для инициализации программного ДСЧ в СКЗИ;

– в образ включены ключевые контейнеры, используемые в работе данного приложения;

• загружать в функционирующий контейнер внешнюю гамму и/или закрытые ключи.

Необходимо:

• Организовать затирание (по окончании сеанса работы СКЗИ) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы СКЗИ. Если это невыполнимо, то гостевая ОС должна использоваться в однопользовательском режиме и на жёсткий диск хостовой машины, а также на образ диска ВМ/контейнера, должны распространяться требования, предъявляемые к ключевым носителям.

• Регулярно устанавливать пакеты обновления безопасности ОС хостовой машины и гостевой ОС (Service Packs, Hot fix и т.п.), обновлять антивирусные базы в соответствии с нормативными документами эксплуатирующей организации. Помимо обновлений для гостевой ОС и гипервизора/демона средств контейнеризации, рекомендуется обновлять инструменты виртуализации, а также утилиты, используемые для управления средой виртуализации. Рекомендуется исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС. Также рекомендуется регулярно знакомится с бюллетенями по безопасности, публикуемыми производителем ПО виртуализации, для получения информации о найденных уязвимостях и их потенциальном влиянии на инфраструктуру виртуализации.

• Исключить возможность попадания в ОС хостовой машины, а также в гостевую ОС программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии.

• Исключить одновременную работу в гостевой ОС с работающим СКЗИ и загруженной ключевой информацией нескольких пользователей. Виртуальная машина, функционирующая под ОС Windows, на которой установлено СКЗИ, должна использоваться только в однопользовательском режиме. В случае невозможности выполнения рекомендации в организации должны быть предусмотрены дополнительные организационные меры по обеспечению сохранности ключевой информации, хранящейся на ВМ/контейнере.

• При использовании СКЗИ в контейнере инициализирующую последовательность ДСЧ (в случае её применения) и ключевые контейнеры размещать в хостовой ОС и «монтировать» к контейнерам.

2.5 Требования к системе управления виртуальной средой/оркестратору контейнеров

Систему управления виртуальной средой/оркестратор контейнеров необходимо выделить в отдельный сетевой сегмент.

В случае подключения системы управления виртуальной инфраструктурой/оркестратора контейнеров к общедоступным сетям передачи данных, должны использоваться дополнительные методы и средства защиты (например, установка межсетевых экранов, IPS/IDS, организация VPN сетей и т.п.).

При использовании СКЗИ в контейнере для инициализации программного ДСЧ в СКЗИ допускается применять инициализирующую последовательность (внешнюю гамму) или «монтировать» к контейнерам физический ДСЧ.

2.6 Требования к миграции образов ВМ/контейнера

При передаче (миграции) образов по каналам связи, выходящим за пределы контролируемой территории, необходимо использовать выделенные каналы или каналы, защищённые средствами шифрования, имеющими сертификат уполномоченного органа. При этом для согласования сеансовых ключей шифрования необходимо использовать криптографические протоколы, обеспечивающие защиту сеансовых ключей и аутентификацию взаимодействующих сторон.

Перед процедурой развертывания контейнера необходимо обеспечить контроль целостности при доставке образа до места эксплуатации.

2.7 Требования к созданию снапшотов

На снапшот ВМ, сделанный после ввода ключевой информации, должны распространяться требования по обращению с ключевыми носителями (раздел 3 документа ЖТЯИ.00101-03 95 01. Правила пользования).

2.8 Требования по защите от сетевых атак

Необходимо:

• в случае подключения ПО виртуализации к общедоступным сетям передачи данных использовать дополнительные методы и средства защиты (например, установка межсетевых экранов, IPS/IDS, организация VPN сетей и т.п.) для блокирования сетевых атак и фильтрации сетевого трафика;

• своевременно устанавливать обновления ПО виртуализации;

• проводить контроль целостности и настроек ПО виртуализации;

• производить регистрацию действий администраторов виртуальной среды;

• запретить информационный обмен между ВМ/контейнерами с использованием общих ресурсов хостовой машины, в том числе общих областей оперативной памяти хостовой машины.

2.9 Контроль целостности ПО виртуальной среды

Необходимо выполнять контроль целостности следующих компонентов виртуальной среды:

- при использовании программно-аппаратных виртуальных сред:
  - ПО гипервизора (на хостовой машине);
  - настроек гипервизора;
  - ПО гостевой ОС;
  - образов ВМ (в т. ч. эталонных образов ВМ), использующихся при развёртывании новых ВМ.
- при использовании виртуальных сред (средств контейнеризации):
  - файловой системы контейнера;
  - ПО средства контейнеризации;
  - ядра хостовой ОС;
  - образов, использующихся при развёртывании новых контейнеров.

Контроль целостности СКЗИ, установленного на ВМ/контейнере, необходимо проводить аналогично контролю целостности СКЗИ, установленного на физической платформе.

2.10 Требования к эталонными образам ВМ/контейнера

При создании эталонных образов ВМ/контейнера предварительно должна быть выполнена проверка:

- соответствия параметров и настроек виртуальной среды установленным требованиям безопасности;
- целостности системного ПО гостевой ОС и ПО СКЗИ в соответствии с эксплуатационной документацией на СКЗИ. После создания эталонного образа должна быть выполнена контрольная установка ВМ/разворачивание контейнера из данного образа и контрольная проверка целостности системного ПО гостевой ОС и ПО СКЗИ.

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

Должна выполняться своевременная установка обновлений безопасности ОС (гостевой и хостовой).

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

Копирование образов ВМ/контейнера с введенной ключевой информацией и/или инициализированным ПДСЧ **запрещено**.

Сборка образа для развертывания контейнеров приложения должна выполняться исключительно Администратором виртуальных машин или Администратором безопасности с учётом выполнения требований, предъявляемых к среде функционирования СКЗИ (подробнее см. разд. 2.4 и раздел 5 документа ЖТЯИ.00101-03 95 01. Правила пользования).

2.11 Требования к аутентификации пользователей СКЗИ

Для аутентификации пользователей СКЗИ допустимо использовать пароли, удовлетворяющие следующим условиям:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.),

а также общепринятые сокращения (USER, ADMIN, ALEX и т. д.);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4-х позициях;
- личный пароль пользователь не имеет права сообщать никому;
- периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 6 месяцев.

2.12 Требование к управлению доступом

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

2.13 Требование к регистрации событий

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

При использовании СКЗИ в контейнере необходимо вести журналы регистрации событий вне контейнера.

2.14 Дополнительные требования при использовании QEMU и Libvirt

При использовании **QEMU** должны выполняться следующие требования:

- конфигурация виртуальной машины QEMU версий 4.2, 5.2, 6.2 не должна содержать эмуляцию EHCI контроллеров USB и паравиртуальных сетевых адаптеров VMWare с поддержкой RDMA;
- конфигурация виртуальной машины QEMU версии 4.2 дополнительно не должна содержать эмуляцию ATI видеоадаптеров;
- удалённый доступ к среде QEMU (посредством протокола QMP) должен быть ограничен для непривилегированных пользователей информационной системы, в составе которой функционирует QEMU;
- виртуальные машины QEMU версий 4.2, 5.2 и 6.2 должны функционировать под управлением ОС Debian 11 и новее, Ubuntu 18.04, 20.04, 21.10 и новее или RHEL 9 и новее.

При использовании **Libvirt** должны выполняться следующие требования:

- виртуальная среда под управлением Libvirt версии 6 должна функционировать под управлением Ubuntu 18.04, 20.04, 21.10 и новее или RHEL 9 и новее;
- при работе виртуальной среды под управлением Libvirt версии 7 данный набор инструментов должен быть обновлён до версии 7.5.0 или выше, или виртуальная среда должна функционировать под управлением Ubuntu 18.04, 20.04, 21.10 и новее или RHEL 9 и новее.

Лист регистрации изменений

Лист регистрации изменений									
№ п/п	Номера листов (страниц)				Всего листов (страниц) в документе	№ документа	Входящий № сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					