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

Средство
Криптографической
Защиты
Информации

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

ЖТЯИ.00101-01 91 09
Листов 12

2019 г

Содержание

Аннотация

Настоящее Руководство дополняет документ ЖТЯИ.00101-01 91 01. Руководство администратора безопасности. Общая часть при использовании СКЗИ в виртуальных средах.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ КриптоПро CSP версия 5.0 КС1 Исполнение 1-Base, должны разрабатываться с учетом требований настоящего документа.

Список определений и сокращений

CRL	Список отозванных сертификатов (Certificate Revocation List)
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ГМД	Гибкий магнитный диск
ДСЧ	Датчик случайных чисел
HDD	Жесткий магнитный диск (Hard Disk Drive)
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
Регистрация	Присвоение определенных атрибутов (адреса, номера ключа, прав использования и т.п.) абоненту
Регламент	Совокупность инструкций и другой регламентирующей документации, обеспечивающей функционирование автоматизированной системы во всех режимах
СВТ	Средства вычислительной техники
Сертификат	Электронный документ, подтверждающий принадлежность открытого ключа или ключа проверки электронной подписи и определенных атрибутов конкретному абоненту
Сертификация	Процесс изготовления сертификата открытого ключа или ключа проверки электронной подписи абонента в центре сертификации
СКЗИ	Средство криптографической защиты информации
СОС	Список отозванных сертификатов (Certificate Revocation List)
СС	Справочник сертификатов открытых ключей и ключей проверки электронной подписи. Сетевой справочник
СФ	Среда функционирования
ЦС	Центр Сертификации (Удостоверяющий Центр)
ЦР	Центр Регистрации
ЭД	Электронный документ
ЭП	Электронная подпись

1 Основные технические данные и характеристики СКЗИ

СКЗИ КриптоПро CSP версии 5.0 КС1 (ЖТЯИ.00101-01) используется в виртуальных средах:

Microsoft Hyper-V Server 2008/2008R2/2012/2012R2/2016 (x64);
Microsoft Hyper-V 8/8.1/10 (x64);
Citrix XenServer 7 (x64);
VMWare WorkStation 11/12/14/15 (x86, x64);
VMWare WorkStation Player 12/14/15 (x86, x64);
VMWare vSphere ESXi/Hypervisor 5.5/6.0/6.5/6.7 (x64);
Oracle VirtualBox 5.2 (x86, x64);
RHEV 4 (x64).

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

2 Требования по защите от НСД

2.1 Организация работ по защите от НСД

Необходимо наличие как минимум двух функциональных ролей виртуальной инфраструктуры:

1) Администратор виртуальных машин, осуществляющий управление компонентами виртуальной инфраструктуры: виртуальными машинами, серверными компонентами, системой хранения данных.

2) Администратор безопасности, осуществляющий администрирование виртуальных машин.

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

2.2 Установка ПО

ПЭВМ, на которых используются средства визуализации и СКЗИ, должны быть допущены для обработки конфиденциальной информации по действующим в Российской Федерации требованиям по защите информации от утечки по техническим каналам, в том числе, по каналу связи (например, СТР-К), с учетом модели угроз в информационной системе заказчика, которым должно противостоять СКЗИ.

Инсталляция СКЗИ на рабочих местах должна производиться только с дистрибутива, полученного по доверенному каналу (раздел 2 ЖТЯИ.00101-01 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 операционных системах:

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

• При установке программного обеспечения виртуализации, гостевой операционной системы и СКЗИ необходимо провести контроль целостности и достоверность соответствующего дистрибутива.

• 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, а также его окружения в соответствии с документацией.

• После завершения процесса создания виртуальной машины, выполнения требуемых настроек и задания требуемых параметров ВМ, должны быть выполнены действия, необходимые для осуществления периодического контроля целостности настроек и параметров ВМ.

Для виртуальных машин VMWare WorkStation, VMWare Player, VMWare Sphere ESX конфигурационный файл находится в той же директории, что и образ виртуальной машины, имеет расширение .vmx. Название конфигурационного файла совпадает с именем виртуальной машины. Аналогично конфигурационные файлы

виртуальных машин Virtual Box лежат в директории с образом виртуальной машины, имеют расширение .vbox и название, совпадающее с именем виртуальной машины. Папкой по умолчанию для хранения настроек виртуальных машин Hyper-V является папка `\ProgramData\Microsoft\Windows\Hyper-V`, имя совпадает с именем виртуальной машины. RHEV по умолчанию хранит конфигурационные файлы в директории `/etc/libvirt/`, имя совпадает с именем виртуальной машины. Для XenServer информация о конфигурации виртуальной машины хранится в специализированной базе мета-данных, дублированной на всех хостах (гипервизоре) XenServer. Администратор, обладающий необходимыми правами, может осуществить экспорт виртуальной машины вместе с метаданными в одном из стандартных форматов — VHD или OVF. Тот же администратор может осуществить резервное копирование метаданных виртуальных машин.

• После завершения процесса установки гостевой ОС должны быть выполнены действия, необходимые для осуществления периодического контроля целостности установленного 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).

2.3 Настройка гипервизора

Настройками гипервизора должно быть обеспечено выполнение следующих требований:

• Для каждой виртуальной машины должна быть выделена отдельная область оперативной памяти хостовой машины.

• Необходимо обеспечить невозможность информационного обмена между виртуальными машинами с использованием общих ресурсов хостовой машины.

• Необходимо обеспечить невозможность информационного обмена между виртуальными машинами, программными процессами и операционной системой 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 виртуальным машинам, и иными программными процессами с использованием общих, разделяемых ресурсов.

2.4 Защита от НСД при эксплуатации СКЗИ

Запрещено:

• оставлять без контроля вычислительные средства, на которых эксплуатируется виртуальная машина с установленным на ней 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 программное обеспечение виртуализации и СКЗИ.

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 виртуальной машины должны распространяться требования, предъявляемые к ключевым носителям.

• регулярно устанавливать пакеты обновления безопасности ОС хостовой машины и гостевой ОС виртуальной машины (Service Packs, Hot fix и т.п.), обновлять антивирусные базы в соответствии с нормативными документами эксплуатирующей организации. Помимо обновлений для гостевой ОС и гипервизора, рекомендуется обновлять инструменты виртуализации, такие как VMware Tools, XenTools,

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, публикуемые производителем гипервизора, для получения информации о найденных уязвимостях и их потенциальном влиянии на инфраструктуру виртуализации.

• исключить возможность попадания в ОС хостовой машины, а также в гостевую систему виртуальной машины 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 данной виртуальной машине.

2.5 Система управления виртуальной средой

Система управления виртуальной средой — это часть виртуальной инфраструктуры, которая с помощью аппаратно-программных средств и средств сетевого взаимодействия обеспечивает:

• 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.

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).

2.6 Требования к миграции образов виртуальных машин

При передаче (миграции) 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, обеспечивающие защиту сеансовых ключей и аутентификацию взаимодействующих сторон.

2.7 Требования к созданию снапшотов

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

2.8 Защита от сетевых атак на гипервизор

Необходимо:

• использовать межсетевые экраны и системы предотвращения вторжений для блокирования сетевых атак и фильтрации сетевого трафика;

• устанавливать обновления ПО гипервизора;

• проводить контроль целостности ПО и настроек гипервизора;

- производить регистрацию действий администраторов виртуальной среды.

2.9 Защита от сетевых атак между ВМ

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

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

2.10 Контроль целостности ПО виртуальной среды

Необходимо выполнять контроль целостности следующих компонентов виртуальной среды:
- ПО гипервизора (на хостовой машине);
- настроек гипервизора;
- ПО гостевой операционной системы;
- образов виртуальных машин, в том числе, эталонных образов ВМ, использующихся при развёртывании новых ВМ.

Контроль целостности СКЗИ, установленного на виртуальной машине, необходимо проводить аналогично контролю целостности СКЗИ, установленного на физической платформе.

2.11 Требования к эталонными загрузочным образам ВМ

При создании эталонных образов виртуальных машин предварительно должна быть выполнена проверка:
- соответствия параметров и настроек ВМ установленным требованиям безопасности;
- целостности системного ПО гостевой ОС и ПО СКЗИ в соответствии с эксплуатационной документацией на СКЗИ. 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;

Для каждого эталонного образа виртуальных машин должны выполняться регламентированные 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 (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 виртуальных машин с введенной ключевой информацией и/или инициализированным ПДСЧ запрещено.

2.12 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.

2.13 Требование к управлению доступом

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

2.14 Требование к регистрации событий

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

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					