

ЗАО «Сигнал-КОМ»

УТВЕРЖДЕН
ШКНР.00046-01 90 03-ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«Крипто-КОМ 3.4»

ПРАВИЛА ПОЛЬЗОВАНИЯ

ШКНР.00046-01 90 03

Листов 20

АННОТАЦИЯ

В данном документе содержатся требования и рекомендации по использованию средства криптографической защиты информации (СКЗИ) «Крипто-КОМ 3.4» в защищенных прикладных системах, оснащенных СКЗИ, и даются рекомендации по организации защиты СКЗИ и ЭВМ от несанкционированного доступа.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих СКЗИ «Крипто-КОМ 3.4», должны разрабатываться с учетом требований настоящего документа.

СОДЕРЖАНИЕ

Аннотация	2
Содержание	3
Введение	4
1. Рекомендации по использованию СКЗИ в защищенных прикладных системах	5
1.1. Конфиденциальность информации	5
1.2. Идентификация и авторство	5
1.3. Целостность	5
1.4. Неотказуемость от передачи электронного документа	5
1.5. Неотказуемость от приема электронного документа	5
1.6. Защита от переповторов	5
1.7. Защита от навязывания информации	5
2. Рекомендации по встраиванию СКЗИ	7
3. Организационно-технические и административные мероприятия при использовании СКЗИ	8
3.1. Организация работ по защите от НСД	8
3.2. Требования по размещению технических средств с установленным СКЗИ	8
3.3. Требования по установке СКЗИ, а также общесистемного и специального ПО на ЭВМ	8
3.4. Требования по защите от НСД при эксплуатации СКЗИ	9
3.5. Обеспечение безопасности функционирования рабочих мест со встроенным СКЗИ	12
4. Использование СКЗИ в виртуальных средах	14
4.1. Организация работ по защите от НСД	14
4.2. Установка программного обеспечения	14
4.3. Настройка гипервизора	15
4.4. Защита от НСД при эксплуатации СКЗИ	15
4.5. Система управления виртуальной средой	16
4.6. Требования к миграции образов виртуальных машин	16
4.7. Требования к созданию мгновенных снимков состояния виртуальной машины	16
4.8. Защита от сетевых атак на гипервизор	16
4.9. Защита от сетевых атак между ВМ	16
4.10. Контроль целостности ПО виртуальной среды	17
4.11. Требования к эталонными загрузочным образам ВМ	17
4.12. Требования к аутентификации пользователей СКЗИ	17
4.13. Требование к управлению доступом	18
4.14. Требование к регистрации событий	18
Приложение. Акт готовности к работе	19
Литература	20

ВВЕДЕНИЕ

Эффективное решение проблем защиты информации требует комплексного подхода, сочетающего в себе криптографические, организационно-технические и административные методы.

При создании защищенных прикладных систем на базе сертифицированных СКЗИ выбор необходимого набора реализуемых криптографических функций и организационно-технических мер определяется в зависимости от модели предполагаемых угроз и требований политики безопасности проектируемой системы.

В разделе 1 настоящего документа приводятся рекомендации по использованию СКЗИ «Крипто-КОМ 3.4» в защищённых прикладных системах.

Раздел 2 настоящего документа содержит рекомендации по встраиванию СКЗИ «Крипто-КОМ 3.4» в защищенные прикладные системы.

Раздел 3 настоящего документа содержит требования и рекомендации в части организационно-технических и административных мероприятий, включая требования по размещению технических средств, использующих СКЗИ в «Крипто-КОМ 3.4», и требования по защите от НСД при установке и эксплуатации СКЗИ.

Раздел 4 настоящего документа содержит требования и рекомендации по использованию СКЗИ в виртуальных средах.

1. РЕКОМЕНДАЦИИ ПО ИСПОЛЬЗОВАНИЮ СКЗИ В ЗАЩИЩЕННЫХ ПРИКЛАДНЫХ СИСТЕМАХ

Настоящий раздел содержит рекомендации по использованию СКЗИ «Крипто-КОМ 3.4» в защищенных прикладных системах.

1.1. Конфиденциальность информации

При передаче данных по информационно-телекоммуникационной сети, а также при хранении данных (на дисках, в базе данных), конфиденциальность обеспечивается использованием функций шифрования.

1.2. Идентификация и авторство

При сетевом взаимодействии (установлении сеанса связи) идентификация и авторство взаимодействующих сторон обеспечивается функциями электронной подписи (ЭП) при использовании их в процессе аутентификации (например, в соответствии с рекомендациями Х.509 [4]). Одновременно при аутентификации должна обеспечиваться защита от повторов. Для этих целей может использоваться функция имитозащиты с вычислением имитовставки на сессионном ключе (симметричный ключ шифрования).

В защищенном электронном документообороте идентификация и авторство обеспечивается использованием функций ЭП электронного документа. Дополнительно должна быть предусмотрена защита от навязывания, повторения электронного документа и целостность справочников ключей проверки ЭП.

1.3. Целостность

Целостность защищаемых данных обеспечивается использованием функций ЭП электронного документа. При использовании функций шифрования (без использования ЭП) целостность данных обеспечивается имитозащитой. Для обеспечения целостности хранимых данных может быть использована функция хеширования или имитозащиты, но при этом не обеспечивается авторство информации.

1.4. Неотказуемость от передачи электронного документа

Неотказуемость от передачи электронного документа обеспечивается подписью документа отправителем с использованием функций ЭП и хранением приемной стороной документа с ЭП в течение установленного срока.

1.5. Неотказуемость от приема электронного документа

Неотказуемость от приема электронного документа обеспечивается использованием функций ЭП и квити́рованием приема документа (подпись квитанции получателем), хранением документа и квитанции с ЭП в течение установленного срока отправляющей стороной.

1.6. Защита от повторения

Защита от повторения обеспечивается использованием криптографических функций ЭП, шифрования или имитозащиты с добавлением уникального идентификатора сетевой сессии (электронного документа) с последующей его проверкой приемной стороной или разработкой специализированного протокола аутентификации (обмена электронными документами).

1.7. Защита от навязывания информации

Защита от нарушителя, навязывающего приемной стороне собственную информацию, переданную якобы от лица санкционированного пользователя (нарушение авторства информации), обеспечивается использованием функций ЭП с проверкой атрибутов электронного документа и ключа проверки ЭП отправителя.

Защита от навязывания информации при компрометации ключа обеспечивается организационно-техническими мероприятиями, например, созданием системы централизованного управления ключевой информацией (оповещением абонентов) или разработкой специализированных протоколов электронного документооборота.

2. РЕКОМЕНДАЦИИ ПО ВСТРАИВАНИЮ СКЗИ

Подробное описание требований, которые должны выполняться при встраивании СКЗИ «Крипто-КОМ 3.4» в высокоуровневые протоколы защиты данных и в защищенные приложения, использующие криптографические функции СКЗИ, приводится в разделе «Требования по встраиванию СКЗИ в приложения» инструкции по встраиванию для соответствующего варианта исполнения СКЗИ.

При встраивании СКЗИ «Крипто-КОМ 3.4» в защищенные прикладные системы с открытым распределением ключей необходимо придерживаться следующих рекомендаций:

- использование открытых ключей (ключей проверки ЭП и открытых ключей ключевого обмена) допускается только в случае достоверного подтверждения их подлинности (отсутствие искажений и принадлежность определенному лицу); выполнение этого условия обеспечивается:
 - заверением открытого ключа третьей доверенной стороной (использование открытого ключа в составе цифрового сертификата, заверенного Удостоверяющим центром (УЦ), или нотариальное заверение копии открытого ключа на бумажном носителе, собственноручно подписанном владельцем ключа);
 - обменом открытыми ключами при личной встрече их владельцев – взаимодействующих сторон;
 - доверенным распространением и хранением открытых ключей в виде справочников и др.;
- в случае использования цифровых сертификатов открытых ключей в качестве третьей доверенной стороны может выступать любой Удостоверяющий центр (УЦ), разработанный с использованием сертифицированного СКЗИ и формирующий сертификаты и списки отозванных сертификатов в соответствии с Рекомендациями ITU-T X.509 [3] и IETF RFC 3280 [4], RFC 4491 [5];
- при каждом использовании сертификата открытого ключа должна выполняться его проверка с помощью сертификата доверенной стороны (УЦ), полученного и хранящегося с использованием процедур, исключающих его подмену, искажение и нештатное использование;
- для исключения возможности использования скомпрометированного или отозванного сертификата, вместе с проверкой подписи УЦ под сертификатом должен выполняться поиск ссылки на данный сертификат в списке отозванных сертификатов и проверка подписи УЦ под списком;
- при работе со справочниками открытых ключей следует придерживаться рекомендаций, изложенных в п.3.1.3 документа [6];
- управление ключевой системой, построенной на базе СКЗИ «Крипто-КОМ 3.4» с использованием цифровых сертификатов, должно выполняться в соответствии с рекомендациями, приведенными в разделе 4 документа [6].

3. ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ И АДМИНИСТРАТИВНЫЕ МЕРОПРИЯТИЯ ПРИ ИСПОЛЬЗОВАНИИ СКЗИ

Защита аппаратного и программного обеспечения от НСД при установке и использовании СКЗИ является составной частью общей задачи обеспечения безопасности информации в системе, в состав которой входит СКЗИ.

Наряду с применением средств защиты от НСД необходимо выполнение целого ряда мер, включающего в себя организационно-технические и административные мероприятия, связанные с обеспечением правильности функционирования технических средств обработки и передачи информации, а также установление соответствующих правил для обслуживающего персонала, допущенного к работе с конфиденциальной информацией.

В приведенных ниже разделах содержатся основные требования по выполнению указанных мер защиты.

3.1. Организация работ по защите от НСД

Защита информации от НСД должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

Защита информации от НСД должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль должен периодически выполняться администратором безопасности на основе требований документации на средства защиты от НСД.

В организации, эксплуатирующей СКЗИ, должен быть назначен администратор безопасности, на которого возлагаются задачи организации работ по использованию СКЗИ, выработки соответствующих инструкций для пользователей, а также контроль за соблюдением описанных ниже требований.

Правом доступа к рабочим местам с установленными СКЗИ должны обладать только определенные для эксплуатации лица, прошедшие соответствующую подготовку. Администратор безопасности должен ознакомить каждого пользователя, применяющего СКЗИ, с документацией на СКЗИ, а также с другими нормативными документами, созданными на её основе.

3.2. Требования по размещению технических средств с установленным СКЗИ

При размещении технических средств с установленным СКЗИ:

- Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых размещены технические средства с установленным СКЗИ, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях.
- Внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений, включая ключевую информацию.
- Размещение СКЗИ в помещениях, в которых осуществляется обработка информации, содержащей сведения, составляющие государственную тайну, осуществляется установленным порядком.

3.3. Требования по установке СКЗИ, а также общесистемного и специального ПО на ЭВМ

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

При установке программного обеспечения СКЗИ следует:

- На технических средствах, предназначенных для работы с СКЗИ использовать только лицензионное программное обеспечение фирм-изготовителей.
- В случае, если в модели угроз, которым должно противостоять СКЗИ в информационной системе заказчика, признана опасной утечка по техническим каналам, ЭВМ, на которых устанавливается СКЗИ, должны быть допущены для обработки информации по действующим в Российской Федерации требованиям по защите информации от утечки по техническим каналам, в том числе, по каналу связи (например, СТР-К). При подключении ПЭВМ с установленным СКЗИ к каналам связи, выходящим за пределы контролируемой территории, защита канала связи должна обеспечиваться применением оптических развязывающих устройств.
- Установка СКЗИ на рабочих местах должна производиться только с дистрибутива, полученного по доверенному каналу.
- При установке ПО СКЗИ на ЭВМ должен быть обеспечен контроль целостности и достоверность дистрибутива СКЗИ и совместно поставляемых с СКЗИ компонент среды функционирования (СФ).
- На ЭВМ 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.
- Предусмотреть меры, исключающие возможность несанкционированного необнаруживаемого изменения аппаратной части технических средств, на которых установлены СКЗИ (например, путем опечатавания системного блока и разъемов ЭВМ).
- 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 (см. [1]).
- Программное обеспечение, устанавливаемое на ЭВМ с СКЗИ, не должно содержать возможностей, позволяющих:
 - модифицировать содержимое произвольных областей памяти;
 - модифицировать собственный код и код других подпрограмм;
 - модифицировать память, выделенную для других подпрограмм;
 - передавать управление в область собственных данных и данных других подпрограмм;
 - несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
 - повышать предоставленные привилегии;
 - модифицировать настройки ОС;
 - использовать недокументированные фирмой-разработчиком функции ОС.

3.4. Требования по защите от НСД при эксплуатации СКЗИ

При организации работ по защите информации от НСД необходимо учитывать следующие требования:

- Необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей в соответствии со следующими правилами:
 - длина пароля должна быть не менее 6 символов при мощности алфавита не менее 10;
 - 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 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.

Указанная политика обязательна для всех учетных записей, зарегистрированных в ОС.

- Средствами BIOS должна быть исключена возможность работы на ЭВМ с СКЗИ, если во время её начальной загрузки не проходят встроенные тесты.
- Запрещается:
 - оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ, после ввода ключевой информации либо иной конфиденциальной информации;
 - вносить какие-либо изменения в программное обеспечение СКЗИ;
 - осуществлять несанкционированное администратором безопасности копирование ключевых носителей;
 - разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации;
 - использовать ключевые носители в режимах, не предусмотренных функционированием СКЗИ;
 - записывать на ключевые носители постороннюю информацию;
 - работать с СКЗИ при неисправности средств защиты от НСД.

Администратор безопасности должен сконфигурировать операционную систему, в среде которой планируется использовать СКЗИ, и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

- Не использовать нестандартные, измененные или отладочные версии ОС.
- Исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой.
- Исключить возможность удаленного управления, администрирования и модификации ОС и её настроек.
- На ЭВМ должна быть установлена только одна операционная система.
- При использовании СКЗИ в виртуальных средах следовать инструкциям, изложенным в п. 4 настоящего документа.
- Правом установки и настройки ОС и СКЗИ должен обладать только администратор безопасности.
- Все неиспользуемые ресурсы системы необходимо отключить (протоколы, сервисы и т.п.).
- Режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень.
- Всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для нормальной работы права.
- Необходимо предусмотреть меры, максимально ограничивающие доступ к следующим ресурсам системы (в соответствующих условиях возможно полное удаление ресурса или его неиспользуемой части):
 - системный реестр;
 - файлы и каталоги;
 - временные файлы;
 - журналы системы;
 - файлы подкачки;
 - кэшируемая информация (пароли и т.п.);
 - отладочная информация.

Кроме того, необходимо организовать затирание (по окончании сеанса работы СКЗИ) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы СКЗИ. Если это не выполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям.

- Должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии.

- Необходимо регулярно устанавливать пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС.
- В случае подключения ЭВМ с установленным СКЗИ к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (например, JavaScript, VBScript, ActiveX), полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети.
- При использовании СКЗИ на ЭВМ, подключенных к общедоступным сетям связи, с целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например: установка межсетевых экранов, организация VPN и т.п.). При этом предпочтение должно отдаваться средствам защиты, имеющим сертификат уполномоченного органа по сертификации.
- Организовать и использовать систему аудита, организовать регулярный анализ результатов аудита.
- СКЗИ должно использоваться со средствами антивирусной защиты, сертифицированными ФСБ России. Класс антивирусных средств защиты определяется условиями эксплуатации СКЗИ в автоматизированных системах.
- Должно быть запрещено использование СКЗИ для защиты речевой информации без проведения соответствующих дополнительных исследований.
- При работе СКЗИ должны быть отключены средства выхода в радиоканал.
- Необходимо проводить перезагрузку ЭВМ с СКЗИ не реже одного раза в неделю.

При использовании СКЗИ в среде ОС Windows 10/Server 2016 для отключения функций телеметрии из системы должны быть удалены служба диагностики (DiagTrack) и сборщики данных (AutoLogger-DiagTrack-Listener), для чего необходимо выполнить следующие действия:

- Проверить наличие и статус сервиса DiagTrack (Панель управления -> Система и безопасность -> Администрирование -> Службы); если сервис запущен, остановить его.
- Удалить запись регистрации сервиса DiagTrack из реестра (удалить папку DiagTrack из раздела HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services).
- Удалить подготовленные к отправке данные, хранящиеся в четырех файлах с расширением *.rbs в директории %ProgramData%\Microsoft\Diagnosis (имена файлов для production сборок ОС – event00.rbs, event01.rbs, event10.rbs и event11.rbs; для insider сборок ОС имена могут отличаться, поэтому необходимо удалить все файлы с расширением *.rbs).
- При возникновении проблем с удалением файла *.rbs необходимо разрешить к нему полный доступ в свойствах на вкладке «Безопасность» и затем удалить файл.
- Остановить автоматическую (AutoLogger) ETW сессию AutoLogger-DiagTrack-Listener, которую DiagTrack активирует в процессесвоей остановки.
- Удалить файл, в который автоматическая (AutoLogger) ETW сессия AutoLogger-DiagTrack-Listener сохраняла собранные данные (путь к файлу хранится в реестровой записи AutoLogger-DiagTrack-Listener в значении FileName; в настоящее время данные сохраняются в файл %ProgramData%\Microsoft\Diagnosis\ETLLogs\AutoLogger\AutoLogger-DiagTrack-Listener.etl).
- Удалить запись регистрации конфигурации автоматической (AutoLogger) ETW сессии AutoLogger-DiagTrack-Listener из реестра (конфигурация сессии хранится под записью AutoLogger-DiagTrack-Listener в разделе реестра HKLM\SYSTEM\CurrentControlSet\Control\WMI\AutoLogger для конфигураций автоматических (AutoLogger) ETW сессий).

- Указанные выше действия необходимо выполнять после каждого кумулятивного обновления Windows 10/Server 2016, поскольку данные обновления фактически приводят к полной переустановке ОС и удаленные сервисы восстанавливаются..

Для всех исполнений СКЗИ «Крипто-КОМ 3.4» для любого используемого механизма аутентификации должно быть ограничено количество подряд следующих попыток аутентификации одного субъекта доступа, число которых не может быть больше 10. При превышении установленного предельного числа подряд следующих попыток аутентификации одного субъекта доступ этого субъекта должен блокироваться на промежуток времени, определяемый условиями эксплуатации СКЗИ в конкретной автоматизированной системе, но не менее чем на 30 секунд.

Исполнения СКЗИ «Крипто-КОМ 3.4», имеющие сертификат соответствия требованиям ФСБ России к СКЗИ класса КС1, при условии выполнения настоящих рекомендаций обеспечивают защиту конфиденциальной информации от внешнего нарушителя, самостоятельно осуществляющего создание методов и средств реализации атак, а также самостоятельно реализующего атаки.

Исполнения СКЗИ «Крипто-КОМ 3.4», имеющие сертификат соответствия требованиям ФСБ России к СКЗИ класса КС2, при условии выполнения настоящих рекомендаций и использовании дополнительных средств защиты от НСД обеспечивают защиту конфиденциальной информации также от внутреннего нарушителя, не являющегося пользователем средств вычислительной техники, на которых реализованы СКЗИ, самостоятельно осуществляющего создание методов и средств реализации атак, а также самостоятельно реализующего атаки.

СКЗИ «Крипто-КОМ 3.4» обеспечивают уровень защищенности класса КС2 при совместном использовании с любым программно-аппаратным комплексом (ПАК) защиты от НСД, сертифицированным ФСБ России по требованиям, выдвигаемым к электронным замкам.

При отсутствии реализации ПАК защиты от НСД для требуемой платформы СКЗИ «Крипто-КОМ 3.4» обеспечивает уровень защищенности класса КС2 только при выполнении следующих требований по защите от НСД:

- процессорный блок, устройства загрузки и разъемы ЭВМ должны быть опечатаны;
- конфиденциальная информация не должна храниться в открытом виде;
- на ЭВМ не должны использоваться средства разработки и отладки;
- СКЗИ должно использоваться со средствами защиты от компьютерных вирусов и компьютерных атак, сертифицированными ФСБ России; класс средств защиты от компьютерных вирусов и компьютерных атак определяется условиями эксплуатации СКЗИ в автоматизированных системах.

3.5. Обеспечение безопасности функционирования рабочих мест со встроенным СКЗИ

В данном разделе представлены основные рекомендации по организационно-техническим мерам защиты для обеспечения безопасности функционирования рабочих мест со встроенным СКЗИ.

- Использование шифровальных средств для криптографической защиты информации подлежит лицензированию в соответствии с действующим законодательством РФ.
- Рабочие места, на которые установлены СКЗИ, должны быть аттестованы комиссией. Результаты работы комиссии отражаются в «Акте готовности к работе» (см.).
- Должностные инструкции администратора безопасности (его заместителя) и ответственного исполнителя должны учитывать требования настоящих рекомендаций.
- При каждом включении рабочей станции с установленным СКЗИ необходимо проверять сохранность печатей системного блока и разъемов рабочей станции.
- Санкционированное снятие и установка приспособлений для опечатки системного блока и разъемов рабочей станции с установленным СКЗИ должно фиксироваться в соответствующем журнале.
- ЭВМ должна обладать средствами самотестирования при включении питания, а также средствами контроля уровня питающих напряжений и прерывания работы компьютера при снижении напряжений ниже допустимых пределов. При

эксплуатации ЭВМ с установленным СКЗИ допускается одно промежуточное выключение питания в течение суток при круглосуточном режиме работы.

- При необходимости удаления файлов, которые использовались при работе СКЗИ, реализовать физическое затирание содержимого удаляемых файлов с помощью утилиты wipe из состава СКЗИ [2].
- В случае обнаружения «посторонних» (незарегистрированных) программ, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках работа на АРМ должна быть прекращена. По данному факту должно быть проведено служебное расследование комиссией в составе представителей служб информационной безопасности организации - владельца сети и организации - абонента сети, где произошло нарушение, и организованы работы по анализу и ликвидации негативных последствий данного нарушения.
- Пользователь должен запускать только те приложения, которые разрешены администратором безопасности.
- Криптографические приложения, созданные на базе СКЗИ «Крипто-КОМ 3.4», должны быть выполнены в соответствии с «Инструкцией по встраиванию» для соответствующего варианта исполнения СКЗИ.

Не допускается:

- Использовать режим простой замены ГОСТ 28147-89 для шифрования информации, кроме ключевой.
- Подключать к ЭВМ дополнительные устройства и соединители, не предусмотренные штатной комплектацией.
- Обрабатывать на ЭВМ, оснащенной СКЗИ, информацию, содержащую сведения, составляющие государственную тайну.
- Использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ.
- Осуществлять несанкционированное вскрытие системных блоков ЭВМ.
- Приносить и использовать в помещении, где установлены средства СКЗИ, радиотелефоны и другую радиопередающую аппаратуру (требование носит рекомендательный характер).

4. ИСПОЛЬЗОВАНИЕ СКЗИ В ВИРТУАЛЬНЫХ СРЕДАХ

4.1. Организация работ по защите от НСД

При использовании СКЗИ в виртуальных средах необходимо наличие как минимум двух функциональных ролей виртуальной инфраструктуры:

- администратор виртуальных машин, осуществляющий управление компонентами виртуальной инфраструктуры: виртуальными машинами, серверными компонентами, системой хранения данных;
- 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.

4.2. Установка программного обеспечения

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.

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 загрузке 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 vSphere ESXi 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.

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 обнаруживаемого изменения аппаратной части технических средств, на которых установлены СКЗИ и компоненты виртуальной инфраструктуры (например, путем опечатывания системного блока и разъемов ПЭВМ).

4.3. 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 котором 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.

4.4. Защита от НСД при эксплуатации СКЗИ

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.

При эксплуатации 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. Рекомендуется исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС;
- 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.

4.5. 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).

4.6. 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.

4.7. Требования к созданию мгновенных снимков состояния виртуальной машины

На мгновенный снимок состояния виртуальной машины (snapshot), сделанный после ввода ключевой информации, должны распространяться требования по обращению с ключевыми носителями (см. [6]).

4.8. Защита от сетевых атак на гипервизор

Для защиты 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.

4.9. 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 и VMWare. Необходимо также обеспечить невозможность

подключения по сети виртуальных машин к своей хост-машине (настройками брандмауэра и/или сетевыми политиками) и невозможность чтения дисков хост-машины в виртуальных машинах (настройками виртуальных машин, касающихся доступа к локальным ресурсам).

4.10. 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.

4.11. 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.

4.12. Требования к аутентификации пользователей СКЗИ

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

- длина пароля должна быть не менее 6 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 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.

4.13. 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.

4.14. Требование к регистрации событий

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

ПРИЛОЖЕНИЕ. АКТ ГОТОВНОСТИ К РАБОТЕ

УТВЕРЖДАЮ

(должность)

(наименование учреждения)

(подпись) (Ф.И.О.)

АКТ

готовности к работе _____ с _____
(наименование учреждения) (наименование изделий)
« _____ » _____ 20__ г.

Комиссия в составе председателя _____
(должность) (Ф.И.О.)

и членов _____

назначенная _____ составила настоящий акт о том, что помещение
эксплуатирующего органа _____, размещение _____,
(название) (оборудование)
хранилища ключевых документов, охрана помещений и подготовленность сотрудников к
обслуживанию _____
(оборудование)
соответствуют: _____
(ГОСТ, инструкция, руководящие документы, правила пользования и т.п.)

Комиссия отмечает, что установка ПО вышеупомянутых изделий проведена в соответствии с

(инструкции)
Вывод: комиссия считает, что объект _____ отвечает требованиям
(название объекта)

(название инструкции)

по обеспечению безопасности связи по уровню _____ и может быть введен в действие.

Председатель:

(подпись) (Ф.И.О.)

Члены комиссии

(подпись) (Ф.И.О.)

(подпись) (Ф.И.О.)

(подпись) (Ф.И.О.)

(подпись) (Ф.И.О.)

М.П.

ЛИТЕРАТУРА

1. СКЗИ «Крипто-КОМ 3.4». Программное обеспечение контроля целостности. Руководство пользователя. ШКНР.00046-01 90 05.
2. СКЗИ «Крипто-КОМ 3.4». Утилита для удаления файлов. Руководство пользователя. ШКНР.00046-01 90 06.
3. ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework, June 1997.
4. RFC 3280. Housley, W. Polk, W. Ford, D. Solo, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002
5. RFC 4491. S. Leontiev, D. Shefanovski, Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile, May 2006.
6. СКЗИ «Крипто-КОМ 3.4». Подсистема управления ключевой информацией. Общее описание. ШКНР.00046-01 31 01.