КРИПТОКОМ

УТВЕРЖДЕН
СЕИУ.00009-01 94 - ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«МагПро КриптоПакет» в. 1.0

Правила эксплуатации

СЕИУ.00009-01 94
Листов 11

Литера О

2008

Аннотация

Настоящий документ регламентирует правила эксплуатации программ, входящих в состав рабочего места абонента СКЗИ «МагПро КриптоПакет» в. 1.0.

Содержание

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

1 Требования к пользователям СКЗИ.

Пользователь допускается к работе с СКЗИ только после ознакомления с должностными инструкциями и с документацией на СКЗИ либо на программные комплексы, использующие СКЗИ.

Пользователь СКЗИ должен принять на себя обязательства по нераспространению доверенных ему конфиденциальных сведений (в частности, ключевой информации). Такие обязательства могут включаться непосредственно в текст контракта (договора). Пользователь допускается к работе с СКЗИ после подписания обязательств, определяющих его материальную или иную форму ответственности за возможные нарушения.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

2 Требования к объектам размещения 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.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

3 Требования по установке СКЗИ, а также общесистемного и специального ПО на ПЭВМ.

На технических средствах, предназначенных для работы с СКЗИ, должно использоваться только лицензионное программное обеспечение фирм-изготовителей.

Установка ПО СКЗИ на ПЭВМ должна производиться только с зарегистрированного, защищенного от записи лицензионного носителя.

На ПЭВМ 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 или иным должностным лицом, ответственным за обеспечение информационной безопасности в организации. 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.

Должны быть предусмотреть меры, исключающие возможность несанкционированного необнаруживаемого изменения аппаратной части технических средств, на которых установленны СКЗИ (например, путем опечатывания системного блока и разъемов ПЭВМ).

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.

Программное обеспечение, устанавливаемое на ПЭВМ 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;
- использовать недокументированные фирмой-разработчиком функции ОС.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

4 Требования по организации защиты от несанкционированного доступа.

Защита аппаратного и программного обеспечения от несанкционированного доступа (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.

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 может быть либо периодическим, либо инициироваться по мере необходимости пользователем или администратором безопасности.

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;
- 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.п.);
- 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 1 года.

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

Средствами BIOS должна быть исключена возможность работы на ПЭВМ с СКЗИ, если во время её начальной загрузки не проходят встроенные тесты.

На ПЭВМ должна быть установлена только одна операционная система. Правом установки и настройки ОС и СКЗИ должен обладать только администратор безопасности.

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;
- отключить все неиспользуемые ресурсы системы (протоколы, сервисы и т.п.);
- настроить на максимальный уровень все режимы безопасности, реализованные в ОС;

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

– назначить минимально возможные для нормальной работы права всем пользователям и группам, зарегистрированным в ОС.

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 ОС должна использоваться в однопользовательском режиме и на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям.

Примечание: Под однопользовательским режимом в данном случае подразумевается такой режим, при котором все пользователи данной рабочей станции имеют одинаковый комплект ключевой информации этой рабочей станции.

Необходимо исключить одновременную работу в ОС с работающим СКЗИ и загруженной ключевой информацией нескольких пользователей.

Должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии. В частности, необходимо организовать и использовать комплекс мероприятий антивирусной защиты.

Необходимо регулярно устанавливать пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), обновлять антивирусные базы, а так же исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС.

В случае подключения ПЭВМ с установленным СКЗИ к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (JavaScript, VBScript, ActiveX и т.п.), 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 ПЭВМ, 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 сетей и т.п.). При этом предпочтение должно отдаваться средствам защиты, имеющим сертификат уполномоченного органа по сертификации.

Запрещается оставлять без контроля вычислительные средства, на которых эксплуатируется СКЗИ, после ввода ключевой информации либо иной конфиденциальной информации.

Запрещается вносить какие-либо изменения в программное обеспечение СКЗИ.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

5 Требования к работе с ключевой информацией.

Закрытые ключи пользователя должны размещаться на отчуждаемом носителе (далее по тексту именуемом ключевым носителем). Ключевой носитель должен быть доступен только специально уполномоченному на это сотруднику (владельцу ключей).

Примечание. При использовании СКЗИ для защиты информации в серверных приложениях допускается размещение закрытых ключей на жестком диске компьютера. При этом режим хранения и использования компьютера должен обеспечивать выполнение требований по работе с ключевой информацией, указанных в настоящем разделе.

В случае повреждения или уничтожения ключевого носителя в результате программных и аппаратных сбоев, несчастных случаев и т.п. работоспособность «МагПро КриптоПакет» в. 1.0 будет нарушена. Для возможности максимально быстрого и полного восстановления работоспособности комплекса в подобных ситуациях рекомендуется заблаговременно создавать архивную копию закрытых ключей на резервном ключевом носителе. При этом режим создания и хранения архивных копий должен исключать доступ к этим копиям кого-либо, кроме владельца ключа.

Архивную копию закрытых ключей на резервном носителе рекомендуется создавать сразу по завершении процедуры создания новых ключей.

При создании новых архивных копий предыдущие (ставшие неактуальными) архивные копии должны быть уничтожены. Ключевые носители после удаления с них закрытых ключей и их архивных копий должны использоваться в том же качестве (для хранения новых ключей) либо уничтожаться.

Все носители закрытой ключевой информации и их архивные копии подлежат строгому поэкземплярному учету.

Создание, хранение, использование и уничтожение выведенной из использования ключевой информации должно производится строго в соответствии с должностной инструкцией.

Режим хранения и использования ключевых носителей должен максимально препятствовать компрометации ключей, то есть доступу к ключевому носителю посторонних лиц, либо возникновению условий, при которых такой доступ был возможен. В случае, если компрометация все же произошла, режим хранения и использования ключевых носителей должен гарантировать обнаружение этого факта.

Пользователь несет персональную ответственность за соблюдение режима хранения и использования своих ключевых носителей. О фактах компрометации ключевой информации пользователь должен немедленно поставить в известность ответственных лиц и действовать в соответствии с должностной инструкцией.

Запрещается:

- 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.

Целостность файлов открытых ключей и списков отзывов сертификатов средствами «МагПро КриптоПакет» в. 1.0 не обеспечивается. Поэтому целостность этих файлов должна

обеспечиваться либо средствами приложений, использующих «МагПро КриптоПакет» в. 1.0, либо организационными мерами.

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения

Лист регистрации изменений									
Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий сопроводительного докум. и дата	Подпись	Дата
Изм.	измененных	замененных	новых	аннулированных					

Порядковый № изменения	Подпись лица, ответственного за изменение	Дата внесения изменения