КРИПТОКОМ

УТВЕРЖДЕН
СЕИУ.00009–05 94 - ЛУ

СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
«МагПро КриптоПакет» 4.0

Правила пользования

СЕИУ.00009–05 94
Листов 16

Литера О

2022

Аннотация

Настоящий документ регламентирует правила пользования средства криптографической защиты информации (СКЗИ) «МагПро КриптоПакет» 4.0 и предназначен для всех лиц, причастных к эксплуатации СКЗИ.

Настоящий документ составлен в соответствиями с Технической спецификацией «Информационная технология. Криптографическая защита информации. Состав и содержание правил пользования средств криптографической защиты информации».

Содержание

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

1 Перечень используемых терминов и сокращений

В настоящих Правилах использованы термины и сокращения из следующих документов:

Р 50.1.053-2005. «Информационные технологии. Основные термины и определения в области технической защиты информации»;

ГОСТ Р 50922—2006. Защита информации. Основные термины и определения;

ГОСТ Р 53114—2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

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

2 Назначение СКЗИ и его основные характеристики

Назначение СКЗИ и его основные характеристики приведены в Формуляре СЕИУ.00009–05 30.

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

3 Ключевая система и ключевые документы

3.1 Характеристики ключевой системы

В СКЗИ используется ключевая система с открытым распределением ключей.

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

Могут использоваться следующие ключевые носители:

– файловый накопитель;
– устройство «Вьюга»;
– устройство «Рутокен».

СКЗИ предоставляет программный интерфейс для подключения других типов ключевых носителей. Также в СКЗИ реализована возможность использования ключей в неизвлекаемой памяти сертифицированных устройств, предоставляющих программный интерфейс PKCS#11 (Рутокен ЭЦП, JaCarta и др.).

В случае, если необходимо загрузить ключи в приложение на сервере, к которому невозможно подключить ключевой носитель (ввиду отсутствия физического доступа владельца ключа к серверу или иных причин), в порядке исключения допускается удаленная загрузка закрытого ключа по сети с рабочего места владельца ключа. При этом должны быть выполнены следующие условия:

– на рабочее место владельца ключа должно быть установлено СКЗИ «МагПро КриптоПакет» 4.0 с полным соблюдением требований, предъявляемых настоящими «Правилами пользования»;
– между рабочим местом владельца ключа и сервером средствами СКЗИ «МагПро КриптоПакет» 4.0 должно быть установлено TLS-соединение;
– файл закрытого ключа должен быть зачитан на рабочем месте владельца ключа и передан на сервер по установленному TLS-соединению;
– недопустима запись закрытого ключа в какие-либо временные файлы как на рабочем месте владельца ключа, так и на сервере.

Примечание. Допускается также размещение закрытого ключа на жестком диске компьютера, при этом режим хранения и использования компьютера должен обеспечивать выполнение требований по работе с ключевой информацией, указанных в настоящем разделе.

Допустимый срок действия ключей шифрования и ключей ЭП – не более 1 года 3 месяцев, ключей проверки ЭП – не более 15 лет после окончания срока действия соответствующих ключей ЭП.

3.2 Управление ключевой информацией

Закрытые и парные им открытые ключи вырабатываются самим владельцем ключа или уполномоченным сотрудником с использованием средств, входящих в состав СКЗИ, имеющего действующий сертификат ФСБ России, либо могут быть получены в аккредитованном Удостоверяющем центре.

После выработки, но до ввода в эксплуатацию открытый ключ должен пройти обязательную сертификацию в Удостоверяющем Центре, сертифицированном по классу не ниже уровня защиты СКЗИ, либо средствами самого СКЗИ.

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

По истечении срока годности ключей их использование должно быть прекращено (за исключением сертификата ключа проверки электронной подписи, который допускается использовать в течение всего срока действия сертификата).

Файлы сертификатов открытых ключей и списков отзыва не содержат закрытой информации и могут располагаться на жестком диске компьютера. При этом должна быть обеспечена защита корневых сертификатов от искажения и подмены.

При каждом использовании сертификата ключа подписи или ключа обмена должна проводиться проверка сертификата с помощью открытого ключа подписи УЦ и проверка, что данный сертификат не является отозванным.

В случае повреждения или уничтожения ключевого носителя в результате программных и аппаратных сбоев, несчастных случаев и т.п. работоспособность «МагПро КриптоПакет» 4.0 будет нарушена. Для возможности максимально быстрого и полного восстановления работоспособности комплекса в подобных ситуациях рекомендуется заблаговременно создавать архивную копию закрытого ключа на резервном ключевом носителе. При этом режим создания и хранения архивных копий должен исключать доступ к этим копиям неуполномоченных лиц.

Архивную копию закрытого ключа на резервном носителе рекомендуется создавать сразу по завершении процедуры создания новых ключей или смены ключей.

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

Все ключевые носители и их архивные копии подлежат строгому поэкземплярному учету.

Смена ключей должна производиться не реже одного раза в год.

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, в том числе при транспортировке ключевых документов из УЦ до ПЭВМ. О фактах компрометации ключевой информации пользователь должен немедленно прекратить использование скомпрометированного ключа и поставить в известность УЦ, выдавший сертификат, либо сотрудника организации, осуществляющего выпуск сертификатов средствами «МагПро КриптоПакет» 4.0.

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

4 Порядок распространения и учета СКЗИ

4.1 Способы передачи и хранения СКЗИ

Предусмотрены три способа передачи экземпляров СКЗИ от Изготовителя к конечным пользователям.

1. Дистрибутивы СКЗИ передаются конечным пользователям на компакт-дисках однократной записи или иных защищённых от записи дистрибутивных носителях и сопровождаются распечатанным формуляром. Формуляр должен быть подписан ответственным сотрудником Изготовителя СКЗИ и заверен печатью Изготовителя. Дистрибутивы СКЗИ и формуляры передаются конечным пользователям напрямую от Изготовителя или через дилеров, имеющих лицензию на распространение СКЗИ.
2. Дистрибутивы СКЗИ и формуляры передаются пользователям в электронном виде. Формуляр заверен усиленной квалифицированной электронной подписью Изготовителя. Дистрибутив или утилита `gost12sum` из состава дистрибутива заверены усиленной квалифицированной электронной подписью Изготовителя.
3. (этот способ возможен только при обновлении уже имеющегося СКЗИ «МагПро КриптоПакет» версии 3.0 или 4.0) Дистрибутив передаётся пользователю в электронном виде, формуляр на бумаге, подписанный ответственным сотрудником Изготовителя и заверенный печатью Изготовителя.

При приёмке СКЗИ в случае получения дистрибутива по способу № 1 конечный пользователь должен проверить:

- целостность упаковки;
- комплектность (наличие дистрибутива и формуляра);
- идентичность учётных номеров СКЗИ на дистрибутиве и в формуляре;
- целостность полученного дистрибутива путём вычисления контрольных сумм файлов дистрибутива с использованием входящей в комплект поставки утилиты `gost12sum` и сравнения вычисленных контрольных сумм с зафиксированными в формуляре.

При приёмке СКЗИ в случае получения дистрибутива по способу № 2 конечный пользователь должен:

- проверить корректность электронной подписи Изготовителя под дистрибутивом (или программы `gost12sum`) и формуляром с помощью имеющегося у конечного пользователя средства с действующим сертификатом ФСБ России;
- распечатать формуляр;
- в случае, если заверен не весь дистрибутив, а только программа `gost12sum`, целостность полученного дистрибутива проверить путём вычисления контрольной суммы архива дистрибутива с использованием утилиты `gost12sum` и сравнения вычисленной контрольной суммы с зафиксированной в формуляре;
- записать дистрибутив на компакт-диск или иной защищённый от записи носитель, надписать на нём учетный номер СКЗИ, указанный в формуляре.

При приёмке СКЗИ в случае получения дистрибутива по способу № 3 конечный пользователь должен:

- проверить целостность полученного дистрибутива путём вычисления контрольной суммы архива дистрибутива и сравнения вычисленной контрольной суммы с зафиксированной в формуляре. Для вычисления контрольных сумм должна использоваться утилита `gost12sum` из состава уже имеющегося СКЗИ «МагПро КриптоПакет» версии 3.0 или 4.0.

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

– записать дистрибутив на компакт-диск или иной защищённый от записи носитель, надписать на нём учетный номер СКЗИ, указанный в формуляре.

Дистрибутив и формуляр должны храниться в подразделении организации, ответственном за эксплуатацию СКЗИ.

4.2 Поэкземплярный учет СКЗИ

В организации, эксплуатирующей «МагПро КриптоПакет» 4.0, должен быть налажен поэкземплярный учёт СКЗИ. При организации поэкземплярного учёта необходимо руководствоваться нормативными документами ФСБ России.

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

5 Требования по обеспечению безопасности при вводе СКЗИ в эксплуатацию

5.1 Требования к встраиванию СКЗИ в прикладные системы и к проведению исследований СФ СКЗИ

Исполнения 3-8 являются функционально законченными изделиями, при их использовании не требуется проводить работы по оценке влияния среды функционирования на СКЗИ.

Исполнения 1-2 предназначены для встраивания в прикладные системы, для которых должны проводиться отдельные тематические исследования.

5.2 Требования по размещению

Требования не предъявляются

5.3 Требования к персоналу, обслуживающему СКЗИ

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 приведенных в документации требований.

Организации, которые используют «МагПро КриптоПакет» 4.0 исключительно в клиентской конфигурации для подключения к внешним сервисам, могут не назначать администратора безопасности и должны пользоваться инструкциями по работе с СКЗИ, полученными от того сервиса, для подключения к которому используется СКЗИ.

Правом доступа к рабочим местам с установленными СКЗИ должны обладать только лица, допущенные к эксплуатации СКЗИ.

5.4 Инициализация и ввод СКЗИ в эксплуатацию

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

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

На ПЭВМ, на которую устанавливается СКЗИ, следует исключить установку средств разработки ПО и отладчиков. 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.

При использовании СКЗИ совместно с АПМДЗ средствами используемого АПМДЗ должна быть обеспечена аутентификация пользователя до загрузки ОС. При этом необходимо организационно запретить сотрудникам, эксплуатирующим СКЗИ, оставлять без присмотра во включенном состоянии ПЭВМ, на которой установлено СКЗИ.

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

После завершения процесса установки следует выполнить действия, необходимые для осуществления периодического контроля целостности установленного СКЗИ, а также его окружения (см. раздел 6.3).

Из программного обеспечения, устанавливаемого на ПЭВМ с СКЗИ, исключить ПО, содержащее возможности, позволяющие:

- 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.

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

6 Требования по обеспечению безопасности при эксплуатации СКЗИ

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

При организации работ по защите информации от НСД необходимо обеспечить выполнение следующих требований:

Право доступа к рабочим местам с установленным СКЗИ должно предоставляется только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию на СКЗИ.

Средствами BIOS должна быть исключена возможность работы на ПЭВМ 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 копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации;
- использовать ключевые носители в режимах, не предусмотренных функционированием СКЗИ;
- записывать на ключевые носители постороннюю информацию.

Необходимо 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.
- Все неиспользуемые ресурсы операционной системы (протоколы, сервисы и т.п.) необходимо отключить.
- 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.
- Ограничить с учетом выбранной в организации политики безопасности использование пользователями запуска программ по расписанию.
- Отключить сетевые протоколы, которые не используются на данной ЭВМ.
- Ограничить количество неудачных попыток входа в систему.
- Организовать и использовать комплекс мероприятий антивирусной защиты.

Должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибка-

ми ОС, повышать предоставленные привилегии.

Необходимо регулярно устанавливать пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), обновлять антивирусные базы.

В случае подключения ЭВМ с установленным СКЗИ к общедоступным сетям передачи данных необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (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.

6.2 Требования к аутентификации и разграничению доступа

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 6 месяцев.

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

Вход в BIOS ПЭВМ должен быть защищен паролем, к которому предъявляются те же требования, что и к паролю администратора системы. Пароль для входа в BIOS должен быть известен только администратору системы и быть отличным от пароля администратора для входа в систему.

6.3 Требования по обеспечению целостности СКЗИ

Должен осуществляться периодический контроль целостности установленного ПО СКЗИ, а также его окружения. Контроль целостности обеспечивается программными средствами путем вычисления хэш-векторов файлов и сравнения вычисленных хэш-векторов с эталонными значениями.

Перечень модулей СКЗИ, подлежащих контролю целостности, и значения хэш-векторов для них приведены в формуляре на СКЗИ.

Контроль целостности осуществляется с помощью средства контроля целостности integrity, входящего в состав СКЗИ. Средство integrity автоматически определяет перечень системных модулей, влияющих на правильность работы СКЗИ, и вычисляет значения хэш-векторов этих модулей.

Эталонные значения хэш-векторов модулей операционной системы должны быть вычислены при установке СКЗИ. После установки обновлений операционной системы эталонные значения обновленных модулей должны быть перевычислены. При формировании файла эталонных значений хэш-векторов необходимо убедиться в совпадении хэш-векторов для модулей СКЗИ с зафиксированными в формуляре на СКЗИ.

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

Файл эталонных значений хэш-векторов должен храниться на отчуждаемом носителе наравне с ключевой информацией. При осуществлении периодического контроля целостности этот файл должен быть доступен в режиме «только чтение» (компакт-диск, флеш-накопитель с защитой от записи и т.п.).

6.4 Порядок обеспечения работоспособности СКЗИ

Должен осуществляться периодический контроль целостности установленного ПО СКЗИ, а также его окружения (см. раздел 6.3).

При выявлении нарушений целостности модулей СКЗИ или операционной системы необходимо выявить и устранить причины искажения модулей.

Восстановление целостности СКЗИ осуществляется с помощью средств установки СКЗИ или программного комплекса, использующего СКЗИ:

– для Windows – путем повторной установки СКЗИ;
– для unix-подобных ОС – путем повторной установки пакета в режиме «reinstall».

Перед установкой СКЗИ необходимо проверить целостность дистрибутивных пакетов СКЗИ (перечень дистрибутивных пакетов и значения хэш-векторов для них приведены в формуляре на СКЗИ).

Восстановление целостности операционной системы осуществляется в соответствии с рекомендациями ее разработчика.

По завершении процедур восстановления целостности модулей СКЗИ и/или операционной системы должна быть проведена проверка корректности восстановления путем вычисления хэш-векторов модулей и их сравнения с ранее зафиксированными эталонными значениями.

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

7 Требования по обеспечению безопасности при выводе СКЗИ из эксплуатации и передаче в ремонт

При выводе СКЗИ из эксплуатации необходимо выполнить следующие действия:
- деинсталлировать все установленные копии СКЗИ;
- уничтожить (разрезать) дистрибутивный компакт-диск;
- уничтожить (разрезать) формуляр;
- удалить с ключевых носителей все криптографические ключи и их архивные копии. Ключевые носители после удаления с них закрытого ключа и его архивных копий должны использоваться в том же качестве (для хранения новых ключей) либо уничтожаться.

Настоящие правила пользования согласованы с ФСБ России.

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