Приказ ФАПСИ от 13 июня 2001 г. N 152
"Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну"

В соответствии с Федеральным законом от 20 февраля 1995 года N 24-ФЗ "Об информации, информатизации и защите информации"*, Законом Российской Федерации от 19 февраля 1993 года N 4524-1 "О федеральных органах правительственной связи и информации"** и Положением о порядке разработки, производства, реализации и использования средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (Положение ПКЗ-99), утвержденным приказом ФАПСИ от 23 сентября 1999 года N 158, зарегистрированным Министерством юстиции Российской Федерации 28 декабря 1999 года, регистрационный N 2029***, с целью определения порядка организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну приказываю:

Утвердить Инструкцию об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну (прилагается).

Генеральный директор Агентства В.Матюхин

* Собрание законодательства Российской Федерации, 1995, N 8, ст.609.

** Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации, 1993, N 12, ст.423.

*** "Российская газета", 2000, 26 января.

Зарегистрировано в Минюсте РФ 6 августа 2001 г.
Регистрационный N 2848

Приложение
к приказу **ФАПСИ РФ**
от 13 июня 2001 г. N 152

Инструкция
об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну

I. Общие положения

1. Настоящая Инструкция определяет единый на территории Российской Федерации порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием сертифицированных ФАПСИ средств криптографической защиты (шифровальных средств) подлежащей в соответствии с законодательством Российской Федерации обязательной защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.*(1)

Данным порядком рекомендуется руководствоваться также при организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием сертифицированных ФАПСИ средств криптографической защиты*(2) не подлежащей обязательной защите конфиденциальной информации, доступ к которой ограничивается в соответствии с законодательством Российской Федерации или по решению обладателя конфиденциальной информации*(3) (за

исключением информации, содержащей сведения, к которым в соответствии с законодательством Российской Федерации не может быть ограничен доступ).

2. Настоящая Инструкция не регламентирует порядка организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации в учреждениях Российской Федерации за границей.

II. Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации

3. Безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации в сетях конфиденциальной связи*(4) организуют и обеспечивают операторы конфиденциальной связи*(5).

Безопасность хранения и обработки с использованием СКЗИ конфиденциальной информации, передаваемой вне сетей конфиденциальной связи, организуют и обеспечивают лица, имеющие лицензию ФАПСИ*(6).

Лица, оказывающие возмездные услуги по организации и обеспечению безопасности хранения и обработки с использованием СКЗИ конфиденциальной информации, передаваемой вне сетей конфиденциальной связи, должны иметь лицензию ФАПСИ на деятельность по предоставлению услуг в области шифрования информации.

4. Безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации, обладатели которой не имеют лицензий ФАПСИ, лицензиаты ФАПСИ организуют и обеспечивают либо по указанию вышестоящей организации, либо на основании договоров на оказание услуг по криптографической защите конфиденциальной информации.

5. Лицензиаты ФАПСИ несут ответственность за соответствие проводимых ими мероприятий по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации лицензионным требованиям и условиям, эксплуатационной и технической документации к СКЗИ, а также положениям настоящей Инструкции.

При этом лицензиаты ФАПСИ должны обеспечивать комплексность защиты конфиденциальной информации, в том числе посредством применения некриптографических средств защиты.

6. Для разработки и осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ конфиденциальной информации лицензиат ФАПСИ создает один или несколько органов криптографической защиты*(7), о чем письменно уведомляет ФАПСИ.

Допускается возложение функций органа криптографической защиты на специальное структурное подразделение по защите государственной тайны, использующее для этого шифровальные средства.

Количество органов криптографической защиты и их численность устанавливает лицензиат ФАПСИ.

7. Орган криптографической защиты осуществляет:

проверку готовности обладателей конфиденциальной информации к самостоятельному использованию СКЗИ и составление заключений о возможности эксплуатации СКЗИ (с указанием типа и номеров используемых СКЗИ, номеров аппаратных, программных и аппаратно-программных средств, где установлены или к которым подключены СКЗИ, с указанием также номеров печатей (пломбиров), которыми опечатаны (опломбированы) технические средства, включая СКЗИ, и результатов проверки функционирования СКЗИ);

разработку мероприятий по обеспечению функционирования и безопасности применяемых СКЗИ в соответствии с условиями выданных на них сертификатов, а также в соответствии с эксплуатационной и технической документацией к этим средствам;

обучение лиц, использующих СКЗИ, правилам работы с ними;

поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним;

учет обслуживаемых обладателей конфиденциальной информации, а также физических лиц, непосредственно допущенных к работе с СКЗИ*(8);

подачу заявок в ФАПСИ или лицензиату, имеющему лицензию ФАПСИ на деятельность по изготовлению ключевых документов*(9) для СКЗИ, на изготовление ключевых документов или исходной ключевой информации. Изготовление из исходной ключевой информации ключевых документов, их распределение, рассылку и учет;

контроль за соблюдением условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ, сертификатом ФАПСИ и настоящей Инструкцией;

расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению уровня защиты конфиденциальной информации; разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

разработку схемы организации криптографической защиты конфиденциальной информации (с указанием наименования и размещения нижестоящих органов криптографической защиты, если таковые имеются, обладателей конфиденциальной информации, реквизитов договоров на оказание услуг по криптографической защите конфиденциальной информации, а также с указанием типов применяемых СКЗИ и ключевых документов к ним, видов защищаемой информации, используемых совместно с СКЗИ технических средств связи, прикладного и общесистемного программного обеспечения и средств вычислительной техники). Указанную схему утверждает лицензиат ФАПСИ.

8. Обладатели конфиденциальной информации, если они приняли решение о необходимости криптографической защиты такой информации или если решение о необходимости ее криптографической защиты в соответствии с Положением ПКЗ-99 принято государственными органами или государственными организациями, обязаны выполнять указания соответствующих органов криптографической защиты по всем вопросам организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации.

9. Для организации взаимодействия обладателей конфиденциальной информации, безопасность хранения, обработки и передачи по каналам связи которой с использованием СКЗИ организуют и обеспечивают различные лицензиаты ФАПСИ, из созданных этими лицензиатами ФАПСИ органов криптографической защиты выделяется координирующий орган криптографической защиты. Все органы криптографической защиты, образованные этими лицензиатами ФАПСИ, обязаны выполнять указания координирующего органа криптографической защиты по обеспечению такого взаимодействия.

10. Инструкции, регламентирующие процессы подготовки, ввода, обработки, хранения и передачи защищаемой с использованием СКЗИ конфиденциальной информации, должны согласовываться с лицензиатом ФАПСИ. Такие инструкции подготавливаются согласно эксплуатационной и технической документации на соответствующие сети связи, автоматизированные и информационные системы, в которых передается, обрабатывается или хранится конфиденциальная информация, с учетом используемых СКЗИ и положений настоящей Инструкции.

11. Лицензиаты ФАПСИ с учетом особенностей своей деятельности могут разрабатывать методические рекомендации по применению настоящей Инструкции, не противоречащие ее требованиям.

12. Ключевые документы для СКЗИ или исходная ключевая информация для выработки ключевых документов изготавливаются ФАПСИ на договорной основе или лицами, имеющими лицензию ФАПСИ на деятельность по изготовлению ключевых документов для СКЗИ.

Изготовлять ключевые документы из исходной ключевой информации могут координирующий орган криптографической защиты (при его наличии), органы криптографической защиты или непосредственно обладатели конфиденциальной информации, применяя штатные СКЗИ, если такая возможность предусмотрена эксплуатационной и технической документацией к СКЗИ.

13. К выполнению обязанностей сотрудников органов криптографической защиты лицензиатами ФАПСИ допускаются лица, имеющие необходимый уровень квалификации для обеспечения защиты конфиденциальной информации с использованием конкретного вида (типа) СКЗИ.

14. Лиц, оформляемых на работу в органы криптографической защиты, следует ознакомить с настоящей Инструкцией под расписку.

15. Обязанности, возлагаемые на сотрудников органа криптографической защиты, могут выполняться штатными сотрудниками или сотрудниками других структурных подразделений, привлекаемыми к такой работе по совместительству.

16. При определении обязанностей сотрудников органов криптографической защиты лицензиаты ФАПСИ должны учитывать, что безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации обеспечивается:

соблюдением сотрудниками органов криптографической защиты режима конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых СКЗИ и ключевых документах к ним;

точным выполнением сотрудниками органов криптографической защиты требований к обеспечению безопасности конфиденциальной информации;

надежным хранением сотрудниками органов криптографической защиты СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, носителей конфиденциальной информации;

своевременным выявлением сотрудниками органов криптографической защиты попыток посторонних лиц получить сведения о защищаемой конфиденциальной информации, об используемых СКЗИ или ключевых документах к ним;

немедленным принятием сотрудниками органов криптографической защиты мер по предупреждению разглашения защищаемых сведений конфиденциального характера, а также возможной утечки таких сведений при выявлении фактов утраты или недостачи СКЗИ, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

17. Обучение и повышение квалификации сотрудников органов криптографической защиты осуществляют организации, имеющие лицензию на ведение образовательной деятельности по соответствующим программам.

18. Сотрудники органа криптографической защиты должны иметь разработанные в соответствии с настоящей Инструкцией и утвержденные лицензиатом ФАПСИ функциональные обязанности. Объем и порядок ознакомления сотрудников органов криптографической защиты с конфиденциальной информацией определяется обладателем конфиденциальной информации.

Обязанности между сотрудниками органа криптографической защиты должны быть распределены с учетом персональной ответственности за сохранность СКЗИ, ключевой документации и документов, а также за порученные участки работы.

19. Физические лица допускаются к работе с СКЗИ согласно перечню пользователей СКЗИ, утверждаемому соответствующим обладателем конфиденциальной информации. До такого утверждения техническая возможность использования СКЗИ лицами, включенными в данный перечень, должна быть согласована с лицензиатом ФАПСИ.

Лицензиаты ФАПСИ в рамках согласованных с обладателями конфиденциальной информации полномочий по доступу к конфиденциальной информации имеют право утверждать такой перечень в отношении подчиненных им должностных лиц.

20. Пользователи СКЗИ обязаны:

не разглашать конфиденциальную информацию, к которой они допущены, рубежи ее защиты, в том числе сведения о криптоключах;

соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;

сообщать в орган криптографической защиты о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящей

Инструкцией, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

немедленно уведомлять орган криптографической защиты о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

21. Непосредственно к работе с СКЗИ пользователи допускаются только после соответствующего обучения.

Обучение пользователей правилам работы с СКЗИ осуществляют сотрудники соответствующего органа криптографической защиты. Документом, подтверждающим должную специальную подготовку пользователей и возможность их допуска к самостоятельной работе с СКЗИ, является заключение, составленное комиссией соответствующего органа криптографической защиты на основании принятых от этих лиц зачетов по программе обучения.

III. Порядок обращения с СКЗИ и криптоключами к ним. Мероприятия при компрометации криптоключей*(10)

22. Предназначенные для обеспечения безопасности хранения, обработки и передачи по каналам связи конфиденциальной информации СКЗИ, а также ключевые документы к ним не должны содержать сведений, составляющих государственную тайну.

23. В федеральных органах исполнительной власти ключевые документы, СКЗИ с введенными криптоключами относятся к материальным носителям, содержащим служебную информацию ограниченного распространения. При этом должны выполняться требования настоящей Инструкции и иных документов, регламентирующих порядок обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти.

Иным обладателям конфиденциальной информации при обращении с ключевыми документами, СКЗИ с введенными криптоключами необходимо руководствоваться настоящей Инструкцией.

24. Для организации и обеспечения безопасности хранения, обработки и передачи по каналам связи конфиденциальной информации следует использовать СКЗИ, позволяющие реализовать принцип абонентского шифрования и предусматривающие запись криптоключей на электронные ключевые носители многократного (долговременного) использования (дискеты, компакт-диски (CD-ROM), Data Key, Smart Card, Touch Memory и т.п.).

25. При необходимости передачи по техническим средствам связи служебных сообщений, касающихся организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации, соответствующие указания необходимо передавать, только применяя СКЗИ. Передача по техническим средствам связи криптоключей не допускается, за исключением специально организованных систем с децентрализованным снабжением криптоключами.

26. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету по установленным формам в соответствии с требованиями Положения ПКЗ-99. При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются также совместно с соответствующими аппаратными средствами.

Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

Журналы поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (приложения 1, 2 к Инструкции) ведут органы криптографической защиты и обладатели конфиденциальной информации.

27. Все полученные обладателем конфиденциальной информации экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета пользователям СКЗИ, несущим персональную ответственность за их сохранность.

Органы криптографической защиты заводят и ведут на каждого пользователя СКЗИ лицевой счет, в котором регистрируют числящиеся за ним СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы.

28. Если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в СКЗИ, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в техническом (аппаратном) журнале (приложение 3 к Инструкции), ведущемся непосредственно пользователем СКЗИ. В техническом (аппаратном) журнале отражают также данные об эксплуатации СКЗИ и другие сведения, предусмотренные эксплуатационной и технической документацией. В иных случаях технический (аппаратный) журнал на СКЗИ не заводится (если нет прямых указаний о его ведении в эксплуатационной или технической документации к СКЗИ).

29. Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ и (или) сотрудниками органа криптографической защиты под расписку в соответствующих журналах поэкземплярного учета. Такая передача между пользователями СКЗИ должна быть санкционирована соответствующим органом криптографической защиты.

Обладатель конфиденциальной информации с согласия органа криптографической защиты может разрешить передачу СКЗИ, документации к ним, ключевых документов между допущенными к СКЗИ лицами по актам без обязательной отметки в журнале поэкземплярного учета.

30. Пользователи СКЗИ хранят инсталлирующие СКЗИ носители, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в

шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

Пользователи СКЗИ предусматривают также раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих криптоключей.

31. Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. При наличии технической возможности на время отсутствия пользователей СКЗИ указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

32. СКЗИ и ключевые документы могут доставляться фельдъегерской (в том числе ведомственной) связью или со специально выделенными нарочными из числа сотрудников органа криптографической защиты или пользователей СКЗИ, для которых они предназначены, при соблюдении мер, исключающих бесконтрольный доступ к ним во время доставки.

Эксплуатационную и техническую документацию к СКЗИ можно пересылать заказными или ценными почтовыми отправлениями.

33. Для пересылки СКЗИ, ключевые документы должны быть помещены в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия, в особенности на записанную ключевую информацию. СКЗИ пересылают отдельно от ключевых документов к ним. На упаковках указывают орган криптографической защиты или пользователя СКЗИ, для которых эти упаковки предназначены. На упаковках для пользователя СКЗИ делают пометку "Лично". Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения упаковок и оттисков печати.

Оформленную таким образом упаковку, при предъявлении фельдсвязью дополнительных требований, помещают во внешнюю упаковку, оформленную согласно предъявляемым требованиям. До первоначальной высылки (или возвращения) адресату сообщают отдельным письмом описание высылаемых ему упаковок и печатей, которыми они могут быть опечатаны.

34. Для пересылки СКЗИ, эксплуатационной и технической документации к ним, ключевых документов следует подготовить сопроводительное письмо, в котором необходимо указать, что посылается и в каком количестве, учетные номера изделий или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Сопроводительное письмо вкладывают в одну из упаковок.

35. Полученные упаковки вскрывают только в органе криптографической защиты или лично пользователи СКЗИ, для которых они предназначены. Если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или сама упаковка и печать - их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ

к ее содержимому, то получатель составляет акт, который высылает отправителю, а при необходимости информирует об этом соответствующий орган криптографической защиты. Полученные с такими отправлениями СКЗИ и ключевые документы до получения указаний от отправителя и органа криптографической защиты применять не разрешается.

36. При обнаружении бракованных ключевых документов или криптоключей один экземпляр бракованного изделия следует возвратить изготовителю через соответствующий орган криптографической защиты для установления причин происшедшего и их устранения в дальнейшем, а оставшиеся экземпляры хранить до поступления дополнительных указаний от органа криптографической защиты или изготовителя.

37. Лицензиат ФАПСИ, допустивший брак при изготовлении ключевых документов, с целью выявления причин случившегося может обратиться в ФАПСИ для проведения на договорной основе экспертизы бракованных ключевых документов.

38. Получение СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должно быть подтверждено отправителю в соответствии с порядком, указанным в сопроводительном письме. Отправитель обязан контролировать доставку своих отправлений адресатам. Если от адресата своевременно не поступило соответствующего подтверждения, то отправитель должен направить ему запрос и принять меры к уточнению местонахождения отправлений.

39. Заказ на изготовление очередных ключевых документов, их изготовление и рассылку на места использования для своевременной замены действующих ключевых документов следует производить заблаговременно. Указание о вводе в действие очередных ключевых документов может быть дано только после поступления в орган криптографической защиты подтверждений от всех заинтересованных пользователей СКЗИ о получении ими очередных ключевых документов.

40. Рассылка изготавливаемых ФАПСИ ключевых документов или исходной ключевой информации на места использования может производиться федеральными органами правительственной связи и информации. Такая рассылка осуществляется по заявкам органа криптографической защиты или заявкам координирующего органа криптографической защиты (при его наличии) на договорной основе.

41. Неиспользованные или выведенные из действия ключевые документы подлежат возвращению в орган криптографической защиты или по его указанию должны быть уничтожены на месте.

42. Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

Криптоключи (исходную ключевую информацию) стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт-дисков (CD-ROM), Data Key, Smart Card, Touch

Memory и т.п.). Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации. Непосредственные действия по уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к СКЗИ уничтожают путем сжигания или с помощью любых бумагорезательных машин.

43. СКЗИ уничтожают (утилизируют) в соответствии с требованиями Положения ПКЗ-99 по решению обладателя конфиденциальной информации, владеющего СКЗИ, и по согласованию с лицензиатом ФАПСИ.

Намеченные к уничтожению (утилизации) СКЗИ подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом СКЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СКЗИ процедура удаления программного обеспечения СКЗИ и они полностью отсоединены от аппаратных средств.

44. Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций СКЗИ, а также совместно работающее с СКЗИ оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.) разрешается использовать после уничтожения СКЗИ без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно удалена (стерта).

45. Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в соответствующих журналах поэкземплярного учета. В эти же сроки с отметкой в техническом (аппаратном) журнале подлежат уничтожению разовые ключевые носители и ранее введенная и хранящаяся в СКЗИ или иных дополнительных устройствах ключевая информация, соответствующая выведенным из действия криптоключам; хранящиеся в криптографически защищенном виде данные следует перешифровать на новых криптоключах.

46. Разовые ключевые носители, а также электронные записи ключевой информации, соответствующей выведенным из действия криптоключам,

непосредственно в СКЗИ или иных дополнительных устройствах уничтожаются пользователями этих СКЗИ самостоятельно под расписку в техническом (аппаратном) журнале.

Ключевые документы уничтожаются либо пользователями СКЗИ, либо сотрудниками органа криптографической защиты под расписку в соответствующих журналах поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом. При этом пользователям СКЗИ разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. После уничтожения пользователи СКЗИ должны уведомить об этом (телефонограммой, устным сообщением по телефону и т.п.) соответствующий орган криптографической защиты для списания уничтоженных документов с их лицевых счетов. Не реже одного раза в год пользователи СКЗИ должны направлять в орган криптографической защиты письменные отчеты об уничтоженных ключевых документах. Орган криптографической защиты вправе устанавливать периодичность представления указанных отчетов чаще одного раза в год.

Уничтожение по акту производит комиссия в составе не менее двух человек из числа сотрудников органа криптографической защиты. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых ключевых документов, инсталлирующих СКЗИ носителей, эксплуатационной и технической документации. Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делаются отметки в соответствующих журналах поэкземплярного учета.

47. Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ. О выводе криптоключей из действия сообщают в соответствующий орган криптографической защиты. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается, по решению лицензиата ФАПСИ, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а передаваемая информация как можно менее ценной.

48. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной информации, пользователи СКЗИ обязаны сообщать в соответствующий орган криптографической защиты. Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения). В случаях недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

49. Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, передававшейся (хранящейся) с использованием

СКЗИ, организует и осуществляет обладатель скомпрометированной конфиденциальной информации.

50. Порядок оповещения пользователей СКЗИ о предполагаемой компрометации криптоключей и их замене устанавливается соответствующим органом криптографической защиты или ФАПСИ.

IV. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним

51. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним*(11), должны обеспечивать сохранность конфиденциальной информации*(12), СКЗИ, ключевых документов.

При оборудовании спецпомещений должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ.

Перечисленные в настоящей Инструкции требования к спецпомещениям могут не предъявляться, если это предусмотрено правилами пользования СКЗИ, согласованными с ФАПСИ.

52. Спецпомещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ. Спецпомещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие спецпомещений в нерабочее время. Окна спецпомещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

53. Размещение, специальное оборудование, охрана и организация режима в спецпомещениях органов криптографической защиты должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

54. Режим охраны спецпомещений органов криптографической защиты, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает лицензиат ФАПСИ по согласованию, при необходимости, с обладателем конфиденциальной информации, в помещениях которого располагается соответствующий орган криптографической защиты. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать положения настоящей Инструкции.

55. Двери спецпомещений органов криптографической защиты должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода сотрудников и посетителей. Ключи от входных дверей нумеруют, учитывают и выдают сотрудникам органов криптографической защиты под

расписку в журнале учета хранилищ. Дубликаты ключей от входных дверей таких спецпомещений следует хранить в сейфе руководителя органа криптографической защиты. Хранение дубликатов ключей вне помещений органа криптографической защиты не допускается.

56. Для предотвращения просмотра извне спецпомещений органов криптографической защиты их окна должны быть защищены.

57. Спецпомещения органов криптографической защиты, как правило, должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации. Исправность сигнализации периодически необходимо проверять руководителю органа криптографической защиты или по его поручению другому сотруднику этого органа совместно с представителем службы охраны или дежурным по организации с отметкой в соответствующих журналах.

58. Каждый орган криптографической защиты для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей должен иметь необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у сотрудника, ответственного за хранилище. Дубликаты ключей от хранилищ сотрудники хранят в сейфе руководителя органа криптографической защиты.

Дубликат ключа от хранилища руководителя органа криптографической защиты в опечатанной упаковке должен быть передан на хранение должностному лицу, назначаемому лицензиатом ФАПСИ, под расписку в соответствующем журнале.

59. По окончании рабочего дня спецпомещения органа криптографической защиты и установленные в них хранилища должны быть закрыты, хранилища опечатаны. Находящиеся в пользовании ключи от хранилищ должны быть сданы под расписку в соответствующем журнале руководителю органа криптографической защиты или лицу, им уполномоченному (дежурному), которые хранят эти ключи в личном или специально выделенном хранилище.

Ключи от спецпомещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ органа криптографической защиты, в опечатанном виде должны быть сданы под расписку в соответствующем журнале службе охраны или дежурному по организации одновременно с передачей под охрану самих спецпомещений. Печати, предназначенные для опечатывания хранилищ, должны находиться у сотрудников органа криптографической защиты, ответственных за эти хранилища.

60. При утрате ключа от хранилища или от входной двери в спецпомещение органа криптографической защиты замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает руководитель органа криптографической защиты.

61. В обычных условиях спецпомещения органа криптографической защиты, находящиеся в них опечатанные хранилища могут быть вскрыты только сотрудниками органа криптографической защиты.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти спецпомещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено руководителю органа криптографической защиты. Прибывшие сотрудники органа криптографической защиты должны оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации конфиденциальной информации и к замене скомпрометированных криптоключей.

62. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в спецпомещениях пользователей СКЗИ должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ.

На время отсутствия пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае пользователи СКЗИ по согласованию с органом криптографической защиты обязаны предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами в их отсутствие.

63. Режим охраны спецпомещений пользователей СКЗИ, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает обладатель конфиденциальной информации по согласованию с соответствующим органом криптографической защиты. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать положения настоящей Инструкции, специфику и условия работы конкретных пользователей СКЗИ.

64. В спецпомещениях пользователей СКЗИ для хранения выданных им ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у соответствующих пользователей СКЗИ.

65. При утрате ключа от хранилища или от входной двери в спецпомещение пользователя СКЗИ замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает орган криптографической защиты.

66. В обычных условиях опечатанные хранилища пользователей СКЗИ могут быть вскрыты только самими пользователями.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти спецпомещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено руководству обладателя конфиденциальной информации и руководителю органа криптографической защиты. Прибывшие сотрудники органа криптографической защиты должны оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации конфиденциальной информации и к замене скомпрометированных криптоключей.

V. Контроль за организацией и обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации

67. Контроль за организацией и обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации - государственный контроль осуществляют федеральные органы правительственной связи и информации*(13). В ходе государственного контроля изучаются и оцениваются:

организация безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации;

достигнутый уровень криптографической защиты конфиденциальной информации;

условия использования СКЗИ.

68. При организации безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ подлежащей в соответствии с законодательством Российской Федерации обязательной защите конфиденциальной информации государственному контролю подлежит деятельность лицензиатов ФАПСИ, а также обладателей конфиденциальной информации, если необходимость криптографической защиты такой информации в соответствии с Положением ПКЗ-99 определяется государственными органами или государственными организациями.

При организации безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ не подлежащей обязательной защите конфиденциальной информации государственному контролю подлежит деятельность лицензиатов ФАПСИ. Обладатели конфиденциальной информации в этом случае могут быть проверены федеральными органами правительственной связи и информации лишь по их просьбе или с их согласия.

Возможность и форму доступа государственных контрольных органов к содержанию конфиденциальной информации определяет руководитель проверяемой организации.

Сроки и периодичность государственного контроля определяет ФАПСИ.

69. Лицензиаты ФАПСИ обязаны контролировать выполнение обладателями конфиденциальной информации данных им указаний по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации, а также соблюдение

такими обладателями условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ, сертификатом ФАПСИ и настоящей Инструкцией.

70. В целях координации государственного контроля и контроля, проводимого лицензиатами ФАПСИ, федеральные органы правительственной связи и информации могут планировать и проводить проверки совместно с заинтересованными органами криптографической защиты, рекомендовать лицензиатам ФАПСИ объекты проверок.

71. Непосредственный допуск к проверке комиссии или уполномоченного федеральных органов правительственной связи и информации осуществляет руководство проверяемых лиц при предъявлении проверяющими удостоверения (предписания) на право проверки, заверенного печатью, и документов, удостоверяющих личность.

Удостоверения (предписания) на право проверки подписывают генеральный директор ФАПСИ, его заместители, а также по их указанию - руководители федеральных органов правительственной связи и информации. Допуск к проверке возможен на основании указаний этих лиц, переданных по техническим каналам связи.

72. По результатам государственного контроля составляется подробный или краткий акт, справка. С актом проверки (справкой) под расписку должно быть ознакомлено руководство проверяемых лиц. Акт (справку) высылают в соответствующий орган криптографической защиты, координирующий орган криптографической защиты (при его наличии) и федеральный орган правительственной связи и информации. Если в ходе проверки выявлены нарушения требований и условий лицензий и сертификатов ФАПСИ, то федеральные органы правительственной связи и информации сообщают в Лицензионный и сертификационный центр ФАПСИ об этих нарушениях и принятых мерах.

Если в использовании СКЗИ обнаружены недостатки, то лицензиаты ФАПСИ, обладатели конфиденциальной информации обязаны принять безотлагательные меры к устранению вскрытых проверкой недостатков и выполнению рекомендаций, изложенных в акте проверки. Сообщения о принятых мерах должны быть представлены в установленные проверяющими сроки. При необходимости может быть составлен план мероприятий, где предусматривается решение соответствующих вопросов.

73. Органы криптографической защиты (координирующие органы криптографической защиты) должны обобщать результаты всех видов контроля, анализировать причины выявленных недостатков, разрабатывать меры по их профилактике, контролировать выполнение рекомендаций, содержащихся в актах проверок.

74. Если в использовании СКЗИ выявлены серьезные нарушения, из-за чего становится реальной утечка конфиденциальной информации, безопасность которой обеспечивается с использованием СКЗИ, то федеральные органы правительственной связи и информации, лицензиаты ФАПСИ вправе дать указание о немедленном прекращении использования СКЗИ до устранения причин выявленных нарушений. В этом случае федеральные органы правительственной

связи и информации могут направить в Лицензионный и сертификационный центр ФАПСИ представление об отзыве (приостановлении действия) лицензий ФАПСИ.

75. Обладатель конфиденциальной информации вправе обратиться в федеральные органы правительственной связи и информации с просьбой о проведении на договорной основе государственного контроля с целью оценки достаточности и обоснованности принимаемых лицензиатом ФАПСИ мер защиты его конфиденциальной информации.

*(1) Информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, в настоящей Инструкции именуется - конфиденциальная информация.

*(2) Сертифицированные ФАПСИ средства криптографической защиты конфиденциальной информации в настоящей Инструкции именуются - СКЗИ. К СКЗИ относятся:

- реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи, включая СКЗИ;

- реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от несанкционированного доступа к информации при ее обработке и хранении;

- реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и "электронной подписи";

- аппаратные, программные и аппаратно-программные средства, системы и комплексы изготовления и распределения ключевых документов для СКЗИ независимо от вида носителя ключевой информации.

*(3) Обладателями конфиденциальной информации могут быть государственные органы, государственные организации и другие организации независимо от их организационно-правовой формы и формы собственности, индивидуальные предприниматели и физические лица.

*(4) Сети конфиденциальной связи - сети связи, предназначенные для передачи конфиденциальной информации.

*(5) Операторы конфиденциальной связи - операторы связи, предоставляющие на основании лицензии ФАПСИ услуги конфиденциальной связи с использованием СКЗИ.

*(6) Операторы конфиденциальной связи и лица, имеющие лицензию ФАПСИ и не являющиеся операторами конфиденциальной связи, в настоящей Инструкции именуются лицензиаты ФАПСИ.

*(7) Органом криптографической защиты может быть организация, структурное подразделение организации - лицензиата ФАПСИ, обладателя конфиденциальной информации. Функции органа криптографической защиты могут быть возложены на физическое лицо.

*(8) Физические лица, непосредственно допущенные к работе с СКЗИ, в настоящей Инструкции именуются - пользователи СКЗИ.

*(9) В настоящей Инструкции используются следующие понятия и определения:

- **криптографический ключ (криптоключ)** - совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе,

- **ключевая информация** - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока;

- **исходная ключевая информация** - совокупность данных, предназначенных для выработки по определенным правилам криптоключей;

- **ключевой документ** - физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию;

- **ключевой носитель** - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации). Различают разовый ключевой носитель (таблица, перфолента, перфокарта и т.п.) и ключевой носитель многократного использования (магнитная лента, дискета, компакт-диск, Data Key, Smart Card, Touch Memory и т.п.);

- **ключевой блокнот** - набор бумажных ключевых документов одного вида (таблиц, перфолент, перфокарт и т.п.), сброшюрованных и упакованных по установленным правилам.

*(10) Под компрометацией криптоключей в настоящей Инструкции понимается хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

*(11) Помещения, где установлены СКЗИ или хранятся ключевые документы к ним, в настоящей Инструкции именуются - спецпомещения.

*(12) Требования к обеспечению сохранности конфиденциальной информации в спецпомещениях аналогичны требованиям к помещениям, где выполняются работы, связанные с хранением (обработкой) такой информации, и устанавливаются обладателем конфиденциальной информации;

*(13) Под федеральными органами правительственной связи и информации в настоящей Инструкции понимаются главные управления ФАПСИ, управления ФАПСИ в федеральных округах, региональные управления правительственной связи и информации, центры правительственной связи.