УТВЕРЖДЕНЫ

руководством 8 Центра
ФСБ России

21 февраля 2008 года

№ 149/6/6-622

ТИПОВЫЕ ТРЕБОВАНИЯ

по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных

I. Общие положения

1.1. Настоящие Требования определяют порядок организации и обеспечения функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну (далее – криптосредство) в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (далее – информационная система).

1.2. Настоящие Требования разработаны во исполнение:

- Федерального закона "О персональных данных" от 27 июля 2006г. № 152-ФЗ (Статья 19);

- Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного постановлением Правительства РФ от 17 ноября 2007г. №781 (далее – Положение);

- Положения о Федеральной службе безопасности Российской Федерации, утвержденного Указом Президента Российской Федерации от 11 августа 2003 года № 960.

1.3. Настоящие Требования:

- являются обязательными для оператора, осуществляющего обработку персональных данных, а также лица, которому на основании договора оператор поручает обработку персональных данных и (или) лица, которому на основании договора оператор поручает оказание услуг по организации и обеспечению безопасности защиты персональных данных при их обработке в информационной системе с использованием криптосредств. При этом существенным условием договора является обязанность уполномоченного лица обеспечить

конфиденциальность персональных данных и безопасность персональных данных при их обработке в информационной системе в случаях, предусмотренных действующим законодательством;

- распространяются на криптосредства, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, все технические средства которых находятся в пределах Российской Федерации, а также в системах, технические средства которых частично или целиком находятся за пределами Российской Федерации.

- не отменяют требования иных документов, регламентирующих порядок обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти.

Оператор с учетом особенностей своей деятельности может разрабатывать не противоречащие настоящим Требованиям методические рекомендации по их применению.

Используемые для целей настоящих Требований термины и определения приведены в приложении 1.

2. Организация и обеспечение безопасности обработки с использованием шифровальных (криптографических) средств персональных данных

2.1. Безопасность обработки персональных данных с использованием криптосредств организуют и обеспечивают операторы, а также лица, которым на основании договора оператор поручает обработку персональных данных и (или) лица, которым на основании договора оператор поручает оказание услуг по организации и обеспечению безопасности обработки в информационной системе персональных данных с использованием криптосредств.

Обеспечение безопасности персональных данных с использованием криптосредств должно осуществляться в соответствии с:

1) Приказом ФСБ России от 9 февраля 2005 г. № 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005);

2) Постановлением Правительства РФ от 29 декабря 2007 г. № 957 "Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами";

3) Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (№ 149/54-144, 2008 г. ФСБ России),

4) Настоящими Требованиями.

2.2. Операторы несут ответственность за соответствие проводимых ими мероприятий по организации и обеспечению безопасности обработки с использованием криптосредств персональных данных лицензионным требованиям и условиям, эксплуатационной и технической документации к криптосредствам, а также настоящим Требованиям.

При этом операторы должны обеспечивать комплексность защиты персональных данных, в том числе посредством применения некриптографических средств защиты.

2.3. При разработке и реализации мероприятий по организации и обеспечению безопасности персональных данных при их обработке в информационной системе оператор или уполномоченное оператором лицо осуществляет:

- разработку для каждой информационной системы персональных данных модели угроз безопасности персональных данных при их обработке;

- разработку на основе модели угроз системы безопасности персональных данных, обеспечивающей нейтрализацию всех перечисленных в модели угроз;

- определение необходимости использования криптосредств для обеспечения безопасности персональных данных и, в случае положительного решения, определение на основе модели угроз цели использования криптосредств для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных и (или) иных неправомерных действий при их обработке;

- установку и ввод в эксплуатацию криптосредств в соответствии с эксплуатационной и технической документацией к этим средствам;

- проверку готовности криптосредств к использованию с составлением заключений о возможности их эксплуатации;

- обучение лиц, использующих криптосредства, работе с ними;

- поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним, носителей персональных данных;

- учет лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационной системе (пользователи криптосредств);

- контроль за соблюдением условий использования криптосредств, предусмотренных эксплуатационной и технической документацией к ним;

- разбирательство и составление заключений по фактам нарушения условий хранения носителей персональных данных, использования криптосредств, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности

персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

- описание организационных и технических мер, которые оператор обязуется осуществлять при обеспечении безопасности персональных данных с использованием криптосредств при их обработке в информационных системах, с указанием в частности:

а) индекса, условного наименования и регистрационных номеров используемых криптосредств;

б) соответствия размещения и монтажа аппаратуры и оборудования, входящего в состав криптосредств, требованиям нормативной документации и правилам пользования криптосредствами;

в) соответствия помещений, в котором размещены криптосредства и хранится ключевая документация к ним, настоящим Требованиям с описанием основных средств защиты;

г) выполнения Требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

Описание принятых мер должно быть включено в уведомление, предусмотренное частью 1 статьи 22 Федерального закона " О персональных данных".

2.4. Пользователи криптосредств допускаются к работе с ними по решению, утверждаемому оператором. При наличии двух и более пользователей криптосредств обязанности между ними должны быть распределены с учетом персональной ответственности за сохранность криптосредств, ключевой, эксплуатационной и технической документации, а также за порученные участки работы.

2.5. Пользователи криптосредств обязаны:

- не разглашать информацию, к которой они допущены, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах защиты;

- соблюдать требования к обеспечению безопасности персональных данных, требования к обеспечению безопасности криптосредств и ключевых документов к ним;

- сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним;

- немедленно уведомлять оператора о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных.

- сдать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящими Требованиями, при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств;

2.6 Обеспечение функционирования и безопасности криптосредств возлагается на ответственного пользователя криптосредств, имеющего необходимый уровень квалификации, назначаемого приказом оператора (далее – ответственный пользователь криптосредств).

Допускается возложение функций ответственного пользователя криптосредств на:

- одного из пользователей криптосредств;

- на структурное подразделение или должностное лицо (работника), ответственных за обеспечение безопасности персональных данных, назначаемых оператором;

- на специальное структурное подразделение по защите государственной тайны, использующее для этого шифровальные средства.

2.7. Ответственные пользователи криптосредств должны иметь функциональные обязанности, разработанные в соответствии с настоящими Требованиями.

2.8. При определении обязанностей пользователя криптосредств необходимо учитывать, что безопасность обработки с использованием криптосредств персональных данных обеспечивается:

- соблюдением пользователями криптосредств 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 криптосредств и ключевых документах к ним;

- точным выполнением пользователями криптосредств требований к обеспечению безопасности персональных данных;

- надежным хранением эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей информации ограниченного распространения;

- обеспечением принятых в соответствии с Требованиями к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных мер.

- своевременным выявлением попыток посторонних лиц получить сведения о защищаемых персональных данных, об используемых криптосредствах или ключевых документах к ним;

- немедленным принятием мер по предупреждению разглашения защищаемых персональных данных, а также возможной их утечки при выявлении фактов утраты или недостачи криптосредств, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

2.9. Лица, оформляемые на работу в качестве пользователей (ответственных пользователей) криптосредств, должны быть ознакомлены с настоящими Требованиями и другими документами, регламентирующими организацию и обеспечение безопасности персональных данных при их обработке в информационных системах, под расписку и несут ответственность за несоблюдение ими требований указанных документов в соответствии с законодательством Российской Федерации.

2.10. Текущий контроль за организацией и обеспечением функционирования криптосредств возлагается на оператора и ответственного пользователя криптосредств в пределах их служебных полномочий.

2.11. Контроль за организацией, обеспечением функционирования и безопасности криптосредств, предназначенных для защиты персональных данных при их обработке в информационных системах персональных данных, осуществляется в соответствии с действующим законодательством Российской Федерации.

2.12. В случае необходимости взаимодействия операторов информационных систем при использовании криптосредств для обеспечения безопасности обработки персональных данных для организации взаимодействия криптосредств по решению операторов персональных данных выделяется координирующий орган, ответственный за обеспечение безопасности персональных данных, указания которого являются обязательными для всех пользователей криптосредств.

3. Порядок обращения с криптосредствами и криптоключами к ним. Мероприятия при компрометации криптоключей.

3.1. Пользователи криптосредств обязаны:

- не разглашать информацию о ключевых документах;

- не допускать снятие копий с ключевых документов;

- не допускать вывод ключевых документов на дисплей (монитор) ПЭВМ или принтер;

- не допускать записи на ключевой носитель посторонней информации;

- не допускать установки ключевых документов в другие ПЭВМ.

3.2. При необходимости передачи по техническим средствам связи служебных сообщений ограниченного доступа, касающихся организации и обеспечения функционирования криптосредств, указанные сообщения необходимо передавать только с использованием криптосредств. Передача по техническим средствам связи криптоключей не допускается, за исключением специально организованных систем с децентрализованным снабжением криптоключами.

3.3. Криптосредства, используемые для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров.

Перечень индексов, условных наименований и регистрационных номеров криптосредств определяется Федеральной службой безопасности Российской Федерации.

3.4. Используемые или хранимые криптосредства, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету. Рекомендуемые формы приведены в Приложении №2. При этом программные криптосредства должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные криптосредства подключаются к системной шине или к одному из внутренних интерфейсов

аппаратных средств, то такие криптосредства 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.

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

Ответственный пользователь криптосредств заводит и ведет на каждого пользователя криптосредств лицевой счет, в котором регистрирует числящиеся за ними криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы.

3.6. Если эксплуатационной и технической документацией к криптосредствам предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в криптосредствах, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в техническом (аппаратном) журнале, ведущемся непосредственно пользователем криптосредств. В техническом (аппаратном) журнале отражают также данные об эксплуатации криптосредств и другие сведения, предусмотренные эксплуатационной и технической документацией. В иных случаях технический (аппаратный) журнал на криптосредства не заводится (если нет прямых указаний о его ведении в эксплуатационной или технической документации к криптосредствам). Типовая форма технического (аппаратного) журнала приведена в приложении № 3.

3.7 Передача криптосредств, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями криптосредств и (или) ответственным пользователем криптосредств под расписку в соответствующих журналах поэкземплярного учета. Такая передача между пользователями криптосредств должна быть санкционирована ответственным пользователем криптосредств.

3.8. Пользователи криптосредств хранят инсталлирующие криптосредства носители, эксплуатационную и техническую документацию к криптосредствам, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

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

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

3.10. Криптосредства и ключевые документы могут доставляться фельдъегерской (в том числе ведомственной) связью или со специально выделенными оператором ответственными пользователями криптосредств и сотрудниками при соблюдении мер, исключающих бесконтрольный доступ к криптосредствам и ключевым документам во время доставки.

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

3.11. Для пересылки криптосредств и ключевых документов они должны быть помещены в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия, в особенности на записанную ключевую информацию. Криптосредства пересылают отдельно от ключевых документов к ним. На упаковках указывают оператора или ответственного пользователя криптосредств, для которых эти упаковки предназначены. На таких упаковках делают пометку «Лично». Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения упаковок и оттисков печати.

До первоначальной высылки (или возвращения) адресату сообщают отдельным письмом описание высылаемых ему упаковок и печатей, которыми они могут быть опечатаны.

3.12. Для пересылки криптосредств, 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.

3.13. Полученные упаковки вскрывает только оператор или ответственный пользователь криптосредств, 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. Полученные с

такими отправлениями криптосредства и ключевые документы до получения указаний от отправителя применять не разрешается.

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

3.15. Получение криптосредств, 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.

3.16. 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 ответственным пользователем криптосредств только после поступления от всех заинтересованных пользователей криптосредств подтверждения о получении ими очередных ключевых документов.

3.17. Неиспользованные или выведенные из действия ключевые документы подлежат возвращению ответственному пользователю криптосредств или по его указанию должны быть уничтожены на месте.

3.18. 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 криптосредствам, 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 криптосредствам, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

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

3.19. Криптосредства уничтожают (утилизируют) по решению оператора, владеющего криптосредствами, и с уведомлением организации, ответственной в соответствии с ПКЗ-2005 за организацию поэкземплярного учета криптосредств.

Намеченные к уничтожению (утилизации) криптосредства подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом

криптосредства считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к криптосредствам процедура удаления программного обеспечения криптосредств и они полностью отсоединены от аппаратных средств.

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

3.21. Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам. 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 криптосредствах или иных дополнительных устройствах ключевая информация, соответствующая выведенным из действия криптоключам; хранящиеся в криптографически защищенном виде данные следует перешифровать на новых криптоключах.

3.22. Разовые ключевые носители, а также электронные записи ключевой информации, соответствующей выведенным из действия криптоключам, непосредственно в криптосредствах или иных дополнительных устройствах

уничтожаются пользователями этих криптосредств самостоятельно под расписку в техническом (аппаратном) журнале.

Ключевые документы уничтожаются либо пользователями криптосредств, либо ответственным пользователем криптосредств под расписку в соответствующих журналах поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом. При этом пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. После уничтожения пользователи криптосредств должны уведомить об этом (телефонограммой, устным сообщением по телефону и т.п.) ответственного пользователя криптосредств для списания уничтоженных документов с их лицевых счетов.

Уничтожение по акту производит комиссия в составе не менее двух человек из числа лиц, допущенных к пользованию криптосредств. 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 криптосредства 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.

3.23. 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 криптосредствам. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается, по решению ответственного пользователя

криптосредств, согласованного с оператором, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а защищаемая информация как можно менее ценной.

3.24. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшихся (хранящихся) с их использованием персональных данных, пользователи криптосредств обязаны сообщать ответственному пользователю криптосредств и (или) оператору.

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.

3.25. Мероприятия по розыску и локализации последствий компрометации ключевых документов организует и осуществляет оператор.

3.26. Ключевые документы для криптосредств или исходная ключевая информация для выработки ключевых документов изготавливаются ФСБ России на договорной основе или лицами, имеющими лицензию ФСБ России на деятельность по изготовлению ключевых документов для криптосредств.

Изготовлять ключевые документы из исходной ключевой информации могут операторы или ответственные пользователи криптосредств, применяя штатные криптосредства, если такая возможность предусмотрена эксплуатационной и технической документацией к криптосредствам.

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

4.1 Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним (далее - режимные помещения), должны обеспечивать сохранность персональных данных, криптосредств и ключевых документов к ним.

При оборудовании режимных помещений должны выполняться требования к размещению, монтажу криптосредств, а также другого оборудования, функционирующего с криптосредствами.

Перечисленные в настоящем документе требования к режимным помещениям могут не предъявляться, если это предусмотрено правилами пользования криптосредствами, согласованными с ФСБ России.

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

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

4.4. Режим охраны помещений, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает ответственный пользователь криптосредств по согласованию, при необходимости, с оператором, в помещениях которого установлены криптосредства или хранятся ключевые документы к ним. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать положения настоящих Требований.

4.5. Двери спецпомещений 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, имеющим право допуска в режимные помещения, под расписку в журнале учета хранилищ. Дубликаты ключей от входных дверей таких помещений следует хранить в сейфе оператора или ответственного пользователя криптосредствами.

4.6. Для предотвращения просмотра извне режимных помещений их окна должны быть защищены.

4.7. Режимные помещения, как правило, должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации. Исправность сигнализации периодически необходимо проверять ответственному пользователю криптосредств совместно с представителем службы охраны или дежурным по организации с отметкой в соответствующих журналах.

4.8. Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих криптосредства носителей должно быть предусмотрено 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 ответственного пользователя криптосредств. Дубликат ключа от хранилища ответственного пользователя криптосредств в опечатанной упаковке должен быть передан на хранение оператору под расписку в соответствующем журнале.

4.9. По окончании рабочего дня режимное помещение и установленные в нем хранилища должны быть закрыты, хранилища опечатаны. Находящиеся в пользовании ключи от хранилищ должны быть сданы под расписку в соответствующем журнале ответственному пользователю криптосредств или уполномоченному (дежурному), которые хранят эти ключи в личном или специально выделенном хранилище.

Ключи от режимных помещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ режимного помещения, в опечатанном виде должны быть сданы под расписку в соответствующем журнале службы охраны или дежурному по организации одновременно с передачей под охрану самих режимных помещений. Печати, предназначенные для опечатывания хранилищ, должны находиться у пользователей криптосредств, ответственных за эти хранилища.

4.10. При утрате ключа от хранилища или от входной двери в режимное помещение 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 оператор или ответственный пользователь криптосредств.

4.11. В обычных условиях режимные помещения, находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями криптосредств, ответственным пользователем криптосредств или оператором.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному пользователю криптосредств или оператору. Прибывший ответственный пользователь криптосредств должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации персональных данных и к замене скомпрометированных криптоключей.

4.12. Размещение и монтаж криптосредств, а также другого оборудования, функционирующего с криптосредствами, в режимных помещениях 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 криптосредствами.

На время отсутствия пользователей криптосредств указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с ответственным пользователем криптосредств необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

Приложение 1

Основные термины и определения

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Доступ к информации - возможность получения информации и ее использования.

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Контролируемая зона - пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств.

Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания

Криптосредство - шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений,

составляющих государственную тайну. В частности, к криптосредствам относятся средства криптографической защиты информации (СКЗИ) - шифровальные (криптографические) средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну

Модель нарушителя - предположения о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

Модель угроз - перечень возможных угроз.

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Пользователь - лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Режимные помещения - помещения, где установлены криптосредства или хранятся ключевые документы к ним.

Средство защиты информации - техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Шифровальные (криптографические) средства - криптосредства:

а) средства шифрования – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;

б) средства имитозащиты – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;

в) средства электронной цифровой подписи – аппаратные, программные и аппаратно–программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа

электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи;

г) средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;

д) средства изготовления ключевых документов (независимо от вида носителя ключевой информации);

е) ключевые документы (независимо от вида носителя ключевой информации).

Приложение 2

ТИПОВАЯ ФОРМА
журнала поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов

№ п.п.	Наименование криптосредства, эксплуатационной и технической документации к ним, ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя криптосредств	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. пользователя криптосредств, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены криптосредства	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

Приложение 3

ТИПОВАЯ ФОРМА
технического (аппаратного) журнала

№ п.п.	Дата	Тип и регистрационные номера используемых криптосредств	Записи по обслуживанию криптосредств	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				Тип ключевого документа	Серийный, криптографический номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны криптосредств, в которую введены криптоключи	Дата	Подпись пользователя криптосредств	
1	2	3	4	5	6	7	8	9	10