ПРАВИТЕЛЬСТВО КУРГАНСКОЙ ОБЛАСТИ

УПРАВЛЕНИЕ ЗАПИСИ АКТОВ ГРАЖДАНСКОГО СОСТОЯНИЯ КУРГАНСКОЙ ОБЛАСТИ

ПРИКАЗ

06.12.2013 г. № 125

г.Курган

Об обеспечения выполнения требований по использованию и обслуживанию СКЗИ

Во исполнение Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119, а также прочих нормативных документов по защите информации

П Р И К А З Ы В А Ю:

1. Назначить ответственным за эксплуатацию криптографических средств защиты информации в информационных системах персональных данных Управления записи актов гражданского состояния Курганской области главного инженера по обслуживанию информационных систем отдела организации и контроля деятельности органов ЗАГС Управления Алексеева Вячеслава Александровича.
2. Утвердить "Функциональные обязанности пользователя, ответственного за использование криптосредств" согласно приложению 1 к настоящему приказу.
3. Утвердить «Требования по обращению с СКЗИ, технической и эксплуатационной документацией к СКЗИ» согласно приложению 2 к настоящему приказу.
4. Контроль за исполнением настоящего приказа оставляю за собой.

Начальник Управления записи актов
гражданского состояния Курганской области Л.А. Кудимова

Приложение 1 к приказу
Управления записи актов
гражданского состояния
Курганской области
от 06.12.2013 г. № 125

Функциональные обязанности пользователя, ответственного за использование криптосредств

1. Общие положения.

1.1.Настоящий документ разработан в соответствии с положениями документа «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 (ФСБ России, № 149/6/6-622, 2008)» (далее Типовые требования).

1.2.Настоящий документ определяет права и обязанности пользователей, ответственных за использование криптосредств в организации.

1.3.Ответственный пользователь криптосредства назначается приказом руководителя Управления записи актов гражданского состояния Курганской области.

2. Ответственный пользователь криптосредства обязан:

2.1.Вести поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним, носителей персональных данных в журнале.

2.2.Вести учет лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности персональных данных в информационной системе (пользователи криптосредств) в журнале.

2.3.Производить установку и ввод в эксплуатацию криптосредств в соответствии с эксплуатационной и технической документацией к этим средствам.

2.4.Проверять готовность криптосредств к использованию с составлением заключений о возможности их эксплуатации.

2.5.Не разглашать информацию, к которой он допущен, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах защиты.

2.6.Соблюдать требования к обеспечению безопасности персональных данных, требования к обеспечению безопасности криптосредств и ключевых документов к ним.

2.7.Сообщать о ставших ему известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним ответственному за защиту информации.

2.8.Немедленно уведомлять ответственного за защиту информации 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.

2.9.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.

2.10. Выполнять прочие положения, предусмотренные Типовыми требованиями, в полном объеме.

3. Ответственный пользователь криптосредства имеет право:

3.1.Инициировать 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 в соответствии с документом «Положение об организации и проведению работ по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных».

4. Ответственному пользователю запрещается:

4.1 Разглашать информацию, к которой он допущен, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах защиты.

С функциональными обязанностями ознакомлен _____/_____

Приложение 2 к приказу
Управления записи актов
гражданского состояния
Курганской области
от 06.12.2013 г. № 125

Требования по обращению с СКЗИ, технической и эксплуатационной документацией к СКЗИ

1. Общие положения

1.1. Настоящие Требования определяют порядок организации деятельности по использованию и обслуживанию шифровальных (криптографических) средств.

2. Организация деятельности по использованию и обслуживанию шифровальных (криптографических) средств

2.1. Организация деятельности по использованию и обслуживанию шифровальных (криптографических) средств должна осуществляться в соответствии с:

- Приказом ФСБ России от 9 февраля 2005 г. № 66 "Об утверждении о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005);
- "Инструкцией 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", утвержденной Приказом ФАПСИ от 13 июня 2001 г. N 152;
- Настоящими Требованиями.

2.2. При осуществлении деятельности с шифровальными (криптографическими) средствами следует производить:

- 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;
- учет лиц, допущенных к работе с криптосредствами;
- контроль за соблюдением условий использования криптосредств, предусмотренных эксплуатационной и технической документацией к ним;
- разбирательство и составление заключений по фактам нарушения условий использования криптосредств.

2.3. Сотрудники Управления записи актов гражданского состояния Курганской области допускаются к работе с криптосредствами приказом руководителя. Сотрудники, допущенные к работе с криптосредствами, несут персональную ответственность за сохранность криптосредств, ключевой, эксплуатационной и технической документации, а также за порученные участки работы.

2.4. Сотрудники, допущенные к работе с криптосредствами, 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 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 ответственного 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 конфиденциальных 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;

2.5. Обеспечение деятельности связанной с распространением и обслуживанием криптосредств возлагается на ответственного сотрудника, имеющего необходимый уровень квалификации, назначаемого приказом руководителя (далее – ответственный сотрудник).

2.6. Допускается возложение функций ответственного сотрудника на:

- одного из сотрудников;
- на структурное подразделение или должностное лицо (работника), ответственных за обеспечение безопасности конфиденциальных данных, назначаемых руководителем.

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

2.8. При определении обязанностей ответственного сотрудника необходимо учитывать, что безопасность обработки с использованием криптосредств конфиденциальных данных обеспечивается:

- соблюдением сотрудниками, 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 сотрудниками требований к обеспечению безопасности конфиденциальной информации;
- надежным хранением эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей информации ограниченного распространения;
- своевременным выявлением попыток посторонних лиц получить сведения о защищаемых данных, об используемых криптосредствах или ключевых документах к ним;
- немедленным принятием мер по предупреждению разглашения защищаемых конфиденциальных 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 сотрудников, работающих с криптосредствами, должны быть ознакомлены с настоящими Требованиями и другими документами, регламентирующими организацию и обеспечение безопасности конфиденциальных данных, 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 ответственного за защиту информации и ответственного за криптосредства сотрудника в пределах их служебных полномочий.

2.11. Контроль за организацией, обеспечением функционирования и

безопасности криптосредств, предназначенных для защиты конфиденциальных данных осуществляется в соответствии с действующим законодательством Российской Федерации.

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

3.1. Сотрудники, работающие с криптосредствами, 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 конфиденциальных данных, 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. Форма журнала учета утверждается приказом руководителя Управления записи актов гражданского состояния Курганской области. 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 сотрудникам, работающим с криптосредствами и несущим персональную ответственность за их сохранность.

Ответственный сотрудник заводит и ведет на каждого сотрудника, работающего с криптосредствами, 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 сотрудником, работающим с криптосредством. 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 утверждается приказом руководителя Управления записи актов гражданского состояния Курганской области.

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

3.8.Сотрудники, работающие с криптосредствами, 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.

Сотрудники 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 сотрудников указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

3.10. Криптосредства и ключевые документы могут доставляться курьерской, фельдъегерской (в том числе ведомственной) связью или со специально выделенными руководителем 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 организацию или ответственного сотрудника, 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 представитель организации или

ответственный сотрудник 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 сотрудником криптосредств, только после поступления от всех заинтересованных сотрудников, работающих с криптосредствами, подтверждения о получении ими очередных ключевых документов.

3.17. Неиспользованные или выведенные из действия ключевые документы подлежат возвращению ответственному сотруднику 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 организации, владеющей 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 сотрудниками, работающими с этими криптосредствами, самостоятельно под расписку в техническом (аппаратном) журнале.

Ключевые документы уничтожаются либо сотрудниками, работающими с криптосредствами, либо ответственным сотрудником под расписку в соответствующих журналах поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом. При этом сотрудникам разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. После уничтожения сотрудники должны уведомить об этом (телефонограммой, устным сообщением по телефону и т.п.) ответственного сотрудника 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 сотрудника, согласованного с ответственным за защиту информации, 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 конфиденциальных данных, сотрудники обязаны сообщать ответственному сотруднику и (или) ответственному за защиту информации.

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 ответственный сотрудник.

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 ответственные сотрудники, 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 конфиденциальных 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 сотрудник по согласованию, при необходимости, с руководителем. 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 ответственного сотрудника.

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 сотруднику 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 сотрудника. Дубликат ключа от хранилища ответственного сотрудника в опечатанной упаковке должен быть передан на хранение ответственному за защиту информации 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 сотруднику, 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 сотрудников, 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 ответственный за защиту информации или ответственный сотрудник.

4.11. В обычных условиях режимные помещения, находящиеся в них опечатанные хранилища могут быть вскрыты только сотрудниками, ответственным сотрудником или руководителем.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному сотруднику или руководителю.

Прибывший ответственный сотрудник должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации конфиденциальных 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 сотрудников, работающих с криптосредствами, 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 сотрудником необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.