УТВЕРЖДЕНО:
Заведующим МБДОУ д/с №14
_____ Е.И. Чепелевой
Приказ № 144/2
от «06» 09 2021 г

ИНСТРУКЦИЯ
по криптографической защите информации
в муниципальном бюджетном дошкольном образовательном учреждении
детский сад №14 «Центр развития ребенка
«Золотой ключик» г. Белгорода

СОДЕРЖАНИЕ

Обозначения и сокращения 3
1. Общие положения 4
2. Организация и обеспечение безопасности обработки защищаемой информации с использованием криптографических средств 4
3. Порядок обращения с криптосредствами и криптоключами к ним. Мероприятия при компрометации криптоключей. 7
4. Эксплуатация криптосредств и обеспечение безопасности информации при передаче по каналам связи 11
5. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним 12
6. Ответственность за нарушение безопасности информации 13
Приложение 1 14
Приложение 2 15
Приложение 3 16
Приложение 4 17
Приложение 5 18
Приложение 6 19
Приложение 7 20
Приложение 8 21

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящем документе применяются следующие обозначения и сокращения:

АРМ	– автоматизированное рабочее место
ИСПДн	– информационная система персональных данных
МНИ	– машинные носители информации
НЖМД	– носитель на жестких магнитных дисках
НСД	– несанкционированный доступ
ПМВ	– программно-математическое воздействие
ПО	– программное обеспечение
ПЭМИН	– побочные электромагнитные излучения и наводки

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Инструкция по криптографической защите информации в муниципальном бюджетном дошкольном образовательном учреждении детский сад №14 «Центр развития ребенка «Золотой ключик» г. Белгорода (далее – Учреждение) разработана в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технология и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152, Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных персональных данных персональных данных с использованием средств автоматизации.

1.2 Инструкция определяет единый порядок:

организации и обеспечения безопасности функционирования шифровальных (криптографических) средств;

эксплуатации криптосредств;

организации и обеспечения безопасности хранения, обработки и передачи по каналам связи информации, не содержащей сведений, составляющих государственную тайну, подлежащей защите с использованием криптосредств.

1.3 Инструкция является обязательной для исполнения всеми сотрудниками Учреждения.

1.4 Криптосредства с введенными ключами и машинные носители информации с записанной на них ключевой информацией относятся к материальным носителям, содержащим информацию ограниченного доступа. При этом должны выполняться требования настоящей Инструкции и иных документов, регламентирующих порядок обращения с информацией ограниченного доступа и ее носителями.

2. ОРГАНИЗАЦИЯ И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБРАБОТКИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ

2.1 Безопасность обработки защищаемой информации с использованием криптосредств организует и обеспечивает руководитель Учреждения.

2.2 Руководитель Учреждения несет ответственность за соответствие проводимых мероприятий по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи защищаемой информации с использованием криптосредств требованиям действующего законодательства и нормативных актов ФСБ России и ФСТЭК России, лицензионным требованиям и условиям, правилам пользования криптосредствами, эксплуатационной и технической документации к ним, а также требованиям настоящий Инструкции.

2.3 Организация и обеспечение эксплуатации криптосредств, а также разработка и осуществление мероприятий по обеспечению безопасности сбора, ввода, хранения, использования и передачи защищаемой информации с применением криптосредств в Учреждении возлагается на администратора безопасности.

2.4 Задачи администратора безопасности в области криптографической защиты включают в себя:

ведение поэкземплярного учета криптосредств, технической и эксплуатационной документации к ним, правил работы с криптосредствами и ключевых документов (приложение 1);

обеспечение соблюдения принципа персональной ответственности пользователей криптосредств и владельцев ключей шифрования за сохранность криптосредств и ключей

шифрования;

учет пользователей криптосредств (приложение 2);

участие в работе комиссий по аттестации помещений, обучению пользователей, установке и вводу в эксплуатацию криптосредств с оформлением акта (приложение 3);

контроль наличия криптосредств, технической и эксплуатационной документации к ним, правил пользования криптосредств и ключевых документов, а также за соблюдением пользователями криптосредств и владельцами ключей шифрования правил обращения с ними;

организация и осуществление приема-передачи криптосредств в случае смены пользователей;

участие в уничтожении ключевой информации с пользователями криптосредств и владельцами ключей шифрования, а также в удалении ПО криптосредств с АРМ пользователей с составлением актов;

формирование и ведение дела, в которое подшиваются все документы, находящиеся в ведении администратора безопасности, а также журналов, определенных настоящей Инструкцией.

2.5 Общие обязанности администратора безопасности:

соблюдать требования законодательных актов и нормативных документов по обеспечению безопасности защищаемой информации, а также защищаемой информации, полученной от внешних организаций, в том числе сведений о функционировании и порядке обеспечения безопасности применяемых криптосредств, о ключевых носителях и документации к ним;

надежно хранить криптосредства, эксплуатационную и техническую документацию, ключевые документы, правила пользования, МНИ с информацией ограниченного доступа;

выявлять попытки посторонних лиц получить сведения об информации ограниченного доступа, используемых криптосредствах или ключевых документах к ним, а также других методов защиты информации и криптосредств;

принимать меры по предупреждению разглашения защищаемых сведений, возможной утечки таких сведений при выявлении фактов утраты или недостачи криптосредств, ключевых документов к ним, а также удостоверений, пропусков, ключей от помещений, хранилищ, сейфов, индивидуальных хранилищ, личных печатей и т.п.

2.6 Обязанности пользователей криптосредств:

сохранять конфиденциальность информации, которая стала известной в процессе выполнения должностных обязанностей, в том числе сведений о закрытых криптографических ключах, паролях и применяемых криптосредствах, организации хранения, обработки и передачи по каналам связи информации с использованием криптосредств;

хранить ключевую информацию, эксплуатационную документацию к криптосредствам на бумажных и машинных носителях в шкафах (ящиках, хранилищах) индивидуального пользования, в условиях, исключающих бесконтрольный доступ к ним, а также их искажение или несанкционированное уничтожение;

в нерабочее время ключевые носители хранить в запираемом на замок и опечатанном индивидуальном хранилище или сдавать на хранение в опечатанном личной печатью пенале (конверте, коробке) администратору безопасности;

выполнять требования эксплуатационных и регламентирующих документов по обеспечению безопасности защищаемой информации, обрабатываемой с применением криптосредств;

сообщать администратору безопасности о ставших ему известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним;

немедленно сообщать администратору безопасности о фактах утраты криптосредств, эксплуатационной документации и ключевых документов к ним, ключей от помещений, хранилищ, личных номерных печатей, нарушении печатей (наклеек), которыми опечатан системный блок ПЭВМ с установленным криптосредством, компрометации ключевой информации и о других фактах, которые могут привести к разглашению защищаемой информации ограниченного доступа, а также о причинах и условиях возможной утечки такой информации;

в случае временного отсутствия (болезнь, командировка, отпуск и т.д.) ключевые носители и пароль оставить на хранение администратору безопасности;

при передаче ПЭВМ с установленным криптосредством в ремонт (на замену, уничтожение), при переустановке программного обеспечения и т.д. сдавать эксплуатационную документацию к криптосредствам, ключевые носители и документы администратору безопасности. При этом с ПЭВМ администратором безопасности должно быть удалено программное обеспечение криптосредств с сохранением архивов на учтенном машинном носителе и с оформлением акта (под роспись в журнале учета) на уничтожение криптосредств;

при увольнении, переводе на работу, не связанную с использованием криптосредств (изменении функциональных обязанностей, не предусматривающих необходимость использования криптосредств), эксплуатационную документацию к криптосредствам, а также ключевые носители сдать с документальным оформлением (под роспись) администратору безопасности.

2.7 Пользователям криптосредств запрещается:

разглашать закрытую ключевую информацию и другую информацию ограниченного доступа, передавать без разрешения администратора безопасности и расписки другим лицам криптосредства, носители ключевой информации и пароли, выводить закрытую ключевую информацию на монитор и принтер;

вносить какие-либо несанкционированные изменения в криптосредство и в аппаратно-программные средства, работающие совместно с установленным криптосредством и способными влиять на функционирование криптосредства;

изменять настройки криптосредств;

осуществлять вскрытие системных блоков ПЭВМ с установленными криптосредствами, подключать к ним дополнительные устройства без разрешения администратора безопасности;

оставлять без контроля ключевые носители, а также ПЭВМ с установленными криптосредствами при включенном питании;

выводить на монитор информацию ограниченного доступа, обрабатываемую с использованием криптосредств в присутствии лиц, не имеющих к этой информации доступа;

хранить закрытые ключи шифрования в памяти ПЭВМ в незашифрованном виде;

выносить ключевые носители за пределы служебных помещений без разрешения руководителя;

применять скомпрометированные ключи или пароли;

осуществлять несанкционированное копирование ключевой информации;

вставлять ключевой носитель в устройство считывания в режимах, не предусмотренных штатным порядком использования ключевого носителя;

записывать на ключевые носители какую-либо информацию, не предусмотренную правилами пользования на криптосредство;

устанавливать ключевые носители в ПЭВМ других пользователей;

производить записи новых ключей на машинные носители ключевой информации без предварительного уничтожения ранее записанной ключевой информации, если иной порядок не определен эксплуатационной документацией.

В случае обнаружения факта несанкционированного доступа к системным блокам, «посторонних» (незарегистрированных) программ, нарушения целостности программного обеспечения работа на этих технических средствах должна быть прекращена. По данному факту проводится служебное расследование и организуются работы по анализу и ликвидации негативных последствий нарушения.

Владельцы ключей шифрования несут полную ответственность за обеспечение сохранности, неразглашения и нераспространения ключей и ключевой информации.

2.8 К выполнению обязанностей, связанных с организацией применения криптосредств, допускаются администраторы безопасности, обладающие знаниями в области организации криптографической защиты, имеющие необходимый уровень квалификации по обеспечению безопасности хранения, обработки и передачи информации ограниченного доступа с использованием применяемых криптосредств и прошедшие соответствующее обучение.

2.9 Сотрудники проходят обучение с последующим допуском к самостоятельной работе с криптосредствами в соответствии с их должностными обязанностями по заявкам, подписанным руководителем и согласованным с администратором безопасности (приложение 4).

2.10 Обучение пользователей криптосредств в Учреждении возлагается на администратора безопасности. По окончании обучения оформляется заключение о подготовке и допуске к самостоятельной работе с криптосредствами (приложение 5).

3. ПОРЯДОК ОБРАЩЕНИЯ С КРИПТОСРЕДСТВАМИ И КРИПТОКЛЮЧАМИ К НИМ. МЕРОПРИЯТИЯ ПРИ КОМПРОМЕТАЦИИ КРИПТОКЛЮЧЕЙ.

3.1 Для организации и обеспечения безопасности хранения, обработки и передачи по каналам связи защищаемой информации используются криптосредства, реализующие принципы абонентского шифрования. Криптографические ключи применяемых криптосредств записываются и хранятся на НЖМД и/или на электронных ключевых носителях многократного использования (дискеты, компакт-диски, Touch Memory, eToken, Рутокен и т.д.).

3.2 Передача по техническим средствам связи закрытых ключей не допускается, за исключением специально организованных систем, правилами пользования которыми предусматривается управление ключевой системой с использованием технических каналов связи.

3.3 Криптосредства, эксплуатационная и техническая документация, правила пользования и ключевые документы между пользователями не передаются.

На период отсутствия основного пользователя, по приказу руководителя может быть произведена временная передача криптосредств, их эксплуатационной и технической документации, а также правил пользования другому пользователю для обеспечения непрерывности технологического процесса обмена информацией. Ключевые документы при этом передавать категорически запрещается.

Указанная передача осуществляется только через администратора безопасности.

3.4 Хранение ключевых документов администраторами безопасности и пользователями криптосредств должно осуществляться в металлических шкафах (сейфах, отдельных ячейках сейфов) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним.

При хранении носителей с ключевой информацией в одном хранилище с другими документами должно быть обеспечено их обособленное хранение в отдельной упаковке (пенале, пакете), опечатанной личной печатью пользователя, владельца ключей шифрования.

Для исключения одновременной компрометации рабочих (действующих) и резервных ключей (вводимых в действие при компрометации рабочих) должно быть обеспечено их раздельное хранение.

3.5 Аппаратные компоненты криптосредств, а также аппаратные средства, с которыми осуществляется штатное функционирование криптосредств должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания

(опломбирования) криптосредств и аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

3.6 При необходимости работы с одного рабочего места нескольких пользователей каждому пользователю криптосредства должен вырабатываться и выдаваться в установленном порядке индивидуальный набор ключевых документов и паролей.

3.7 Администратором безопасности ведется поэкземплярный учет криптосредств, эксплуатационной и технической документации к ним, правил пользования, ключевых документов, а также осуществляется контроль за их движением с момента поступления (инсталляции) и до уничтожения (деинсталляции, возврата). Основным принципом учета является одноразовость регистрации.

3.8 Основным требованием при организации учета криптосредств, эксплуатационной и технической документации к ним, правил пользования, а также ключевых документов является создание системы регистрации, позволяющей обеспечить персональную ответственность пользователей за их сохранность.

3.9 Сопроводительные письма с приложениями и акты приема-передачи регистрируются порядком, установленным для входящих документов, после чего криптосредства, эксплуатационная и техническая документация к ним, правила пользования и ключевая информация подлежат регистрации в журнале поэкземплярного учета.

На сопроводительных письмах или актах приема-передачи производится отметка о регистрации приложений со ссылками на номер журнала поэкземплярного учета.

3.10 Передача криптосредств, технической и эксплуатационной документации к ним, правил пользования, ключевых документов пользователям, непосредственно отвечающим за дальнейшую работу с ними (обработку, хранение, дальнейшую пересылку, установку, уничтожение и т. д.), производится под роспись в журналах учета или в необходимых случаях по акту с отметкой о номере акта в соответствующем журнале учета.

3.11 Администратором безопасности ведется Журнал поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, правил пользования и ключевых документов, являющийся журналом основного учета по форме, приведенной в приложении 1.

В данном журнале должны быть зарегистрированы все криптосредства, документация и ключевые документы к ним, используемые при организации и осуществлении криптографической защиты в Учреждении, в том числе находящиеся на хранении, предназначенные для пересылки, полученные во временное пользование и т.п.

Учет в Журнале поэкземплярного учета криптосредств других средств защиты, не являющихся криптосредствами, не допускается.

3.12 Маркировка МНИ осуществляется простановкой регистрационного штампа (при наличии возможности) и нанесением следующих реквизитов: учетного номера, даты и росписи лица, проводившего учет и маркировку учетных данных. На ключевых носителях в правом верхнем углу производится пометка «Конфиденциально» или «Для служебного пользования».

При отсутствии возможности (из-за размеров) нанесения всех учетных данных на МНИ (Touch Memory, eToken, флэш-носители и т.п.) разрешается использовать стикеры с проставленными при их изготовлении номерами. В этом случае в журнале учета записывается номер стикера, принадлежащего данному носителю, и заводской номер МНИ (если имеется). Допускается также на такие носители прикреплять специально изготовленные бирки с нанесенными учетными данными, опечатанные пломбиром.

3.13 Отметки об уничтожении записанной на МНИ информации производятся в формах учета, где была зарегистрирована указанная выше информация.

3.14 Если правилами пользования криптоключи вводят и хранят (на весь срок их действия) непосредственно в криптосредстве, то такая электронная запись криптоключа должна быть зарегистрирована в аппаратном журнале учета эксплуатации криптосредств (приложение 6).

3.15 При ведении журналов учета применение подчисток, использование корректирующих

средств и т.п. не допускается.

При необходимости исправления произведенной записи текст, подлежащий исправлению, аккуратно зачеркивается без сокрытия его содержания, и на свободном месте Журнала производится запись: «Зачеркнутое в п.___ в гр. __ «_____» не читать, исправленному на «_____» верить». Запись заверяется подписью лица, ответственного за ведение Журнала.

3.16 Журналы поэкземплярного учета ведутся до полного использования, после чего закрываются в установленном порядке.

Все числящиеся на момент окончания журнала криптосредства, эксплуатационная и техническая документация к ним, правила пользования, ключевые документы берутся на учет во вновь заведенном журнале поэкземплярного учета лицом, ответственным за ведение журнала.

Закрытые производством журналы поэкземплярного учета хранятся в Учреждении 5 лет, после чего уничтожаются по акту.

3.17 При увольнении, переводе на другую работу администратора безопасности дистрибутивы (копии дистрибутивов) криптосредств, техническая, эксплуатационная документация к ним, правила пользования, ключевые носители и документы передаются вновь назначенному администратору безопасности (приложение 7).

3.18 Заказ на изготовление очередных ключевых документов, их изготовление и рассылку на места использования для своевременной замены действующих ключевых документов необходимо производить заблаговременно.

3.19 Уничтожение криптоключей (исходной ключевой информации) может производиться путем физического уничтожения ключевого носителя, на котором они записаны, 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, Data Key, Smart Card, Touch Memory, eToken и т.п.).

Удаление информации с магнитных носителей может осуществляться с использованием систем гарантированного уничтожения информации.

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 типам криптосредств.

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

3.20 Предназначенные к уничтожению (утилизации) криптосредства подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом криптосредства считаются изъятыми (деинсталлированными) из аппаратных средств, если выполнены предусмотренные эксплуатационной и технической документацией к криптосредствам процедуры удаления. Удаление программного обеспечения криптосредств производится администратором безопасности с оформлением акта (под роспись в журнале) на уничтожение криптосредств.

3.21 Уничтожение по акту (приложение 8) производится комиссией в составе не менее двух человек. В состав комиссии в обязательном порядке включается администратор безопасности. В акте указывается, что уничтожается и в каком количестве, серии, учетные номера, экземпляры. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров, уничтожаемых криптосредств, правил пользования, эксплуатационной и технической документации, ключевых документов.

Исправления в тексте акта не допускаются. В случае обнаружения комиссией неточностей в тексте акта в процессе уничтожения, они должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делаются отметки в соответствующих журналах учета.

3.22 О нарушениях, которые могут привести к компрометации криптоключей или передававшейся (хранящейся) с их использованием информации, пользователи криптосредств, владельцы ключей шифрования обязаны сообщать администратору безопасности, от которого были получены ключевые документы.

Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения).

3.23 События, квалифицируемые как явная компрометация ключей:

утрата ключевых дискет;

утрата ключевых дискет с последующим обнаружением;

увольнение работников, имевших доступ к ключевой информации;

нарушение печати на сейфе с ключевыми носителями;

нарушение правил хранения и уничтожения (после окончания срока действия) ключевой информации;

наличие в подписи сертификата, находящегося в списке отозванных;

случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);

навязывание заведомо ложной информации в документах, защищенных имитовставками.

3.24 К событиям, квалифицируемым как подозрение о наличии факта компрометации криптографического ключа, требующим проведения расследования и принятия решения на предмет происшествия явной компрометации, относится возникновение подозрений в утечке информации в системе защищенной связи.

3.25 Основные правила в принятии решения о компрометации:

в случае признания факта компрометации любого из закрытых ключей, записанных на ключевой дискете абонента, признаются непосредственно скомпрометированными все ключи на данной дискете. Данный абонент признается непосредственно скомпрометированным;

в случае признания факта непосредственной компрометации любого из ключей у любого абонента коллектива однозначно признаются скомпрометированными все ключи, общие для абонентов данного коллектива. Пользователи коллектива, не подвергшиеся непосредственной компрометации, признаются косвенно скомпрометированными.

У пользователей коллектива, не подвергшихся непосредственной компрометации, нескомпрометированными могут быть признаны только индивидуальные ключи (персональный ключ, закрытый ключ ЭП, jump-ключ);

в случае признания факта компрометации любого из закрытых ключей, записанных на мастер-дискете администратора, однозначно признаются скомпрометированными все ключи на данной дискете;

в случае признания факта компрометации любого из закрытых ключей, записанных на жестком диске, признаются скомпрометированными все ключи данного АРМа;

в случае компрометации ключей администратора ключевого центра считается скомпрометированной вся ключевая информация в сети.

3.26 При наступлении любого из перечисленных в п. 3.23 событий или подозрении в компрометации ключа пользователь криптосредства должен немедленно прекратить связь с другими пользователями и сообщить о факте компрометации администратору безопасности.

По факту компрометации ключей должно быть проведено служебное расследование. Выведенные из действия скомпрометированные ключи после проведения служебного расследования подлежат уничтожению порядком, определенным настоящей Инструкцией.

3.27 На замену скомпрометированных ключей пользователю криптосредства и владельцу

ключей шифрования администратором безопасности вырабатываются и выдаются новые ключи. Если предусмотрено технологическим процессом, новый ключ вырабатывается пользователем криптосредства самостоятельно.

4. ЭКСПЛУАТАЦИЯ КРИПТОСРЕДСТВ И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ПЕРЕДАЧЕ ПО КАНАЛАМ СВЯЗИ

4.1 При использовании ПЭВМ с установленными криптосредствами, подключенных к информационно-телекоммуникационным сетям общего пользования, с целью исключения возможности несанкционированного доступа к среде функционирования криптосредств, компонентам криптосредств, а также к системным ресурсам используемых операционных систем со стороны указанных сетей должны выполняться требования Указа Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

4.2 На средствах вычислительной техники, подлежащих оснащению криптосредствами, должно использоваться только лицензионное программное обеспечение фирм-производителей.

4.3 Перед установкой криптосредств необходимо проверить программное обеспечение ПЭВМ на отсутствие вирусов и программных закладок. Удаляются все неиспользуемые общие ресурсы на ПЭВМ, в том числе и создаваемые по умолчанию.

4.4 На ПЭВМ не должны устанавливаться средства разработки программного обеспечения и программы-отладчики. Если наличие средства отладки приложений обусловлено технологическими потребностями, то его использование должно быть санкционировано администратором безопасности. При этом должны быть реализованы меры, исключающие возможность использования этих средств, для просмотра и редактирования кода и памяти приложений, использующих криптосредства.

4.5 Для обеспечения защиты от несанкционированного доступа (НСД) используется система парольной защиты.

4.6 При отсутствии возможности применения программно-аппаратных средств защиты от несанкционированного доступа (например, из-за конструктивных особенностей, при удаленных настройке, администрировании, резервном копировании и восстановлении аппаратно-программных комплексов с криптосредствами, работающих без участия, допускается защиту информации от несанкционированного доступа производить за счет дополнительных организационных мер:

- размещение указанных криптосредств в аттестованном, специально выделенном помещении;
- запирание на замок и опечатывание двери в указанное помещение в случае отсутствия необходимости санкционированного доступа в это помещение;
- допуск в указанное помещение только работников, назначенных приказом руководителя. Указанные работники не должны иметь доступа к настройкам криптосредств;
- блокировка разъемов для подключения монитора и манипулятора «мышь»;
- контроль администратором безопасности не реже одного раза в два месяца целостности установленного программного обеспечения с помощью программ контроля целостности, входящих в комплект размещенного в помещении криптосредства;
- установление системы сигнализации с выводом на центральный пункт охраны и круглосуточное видеонаблюдение.

4.7 В случае использования ПЭВМ несколькими операторами с различными ключами необходимо производить выгрузку ключевой информации (перезагрузку ПЭВМ).

5. РАЗМЕЩЕНИЕ, СПЕЦИАЛЬНОЕ ОБОРУДОВАНИЕ, ОХРАНА И ОРГАНИЗАЦИЯ РЕЖИМА В ПОМЕЩЕНИЯХ, ГДЕ УСТАНОВЛЕНЫ КРИПТОСРЕДСТВА ИЛИ ХРАНЯТСЯ КЛЮЧЕВЫЕ ДОКУМЕНТЫ К НИМ

5.1 Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним (далее – спецпомещения), должны обеспечивать сохранность информации ограниченного доступа, криптосредств и ключевых документов.

5.2 Перечисленные в настоящей Инструкции требования к спецпомещениям могут не предъявляться, если это предусмотрено правилами пользования криптосредствами, согласованными с ФСБ России.

5.3 При оборудовании спецпомещений должны выполняться требования к размещению и установке криптосредств, а также других средств, совместно функционирующих с криптосредствами, предусмотренные правилами пользования.

5.4 Помещения, в которых размещены криптосредства, должны иметь прочные входные двери с замками, гарантирующими надежное закрытие дверей в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно несанкционированное проникновение в помещения посторонних лиц, должны быть оборудованы металлическими решетками (ставнями) или тремя рубежами охранной сигнализации.

5.5 Работоспособность охранной сигнализации проверяется ответственным работником при сдаче помещения под охрану. Исправность охранной сигнализации ежемесячно проверяется администратором безопасности совместно с представителем службы эксплуатации здания или дежурным из службы охраны с отметкой в соответствующем журнале контроля состояния охранно-пожарной сигнализации.

5.6 Размещение, оборудование, охрана и организация режима работы в спецпомещениях должны исключить возможность неконтролируемого проникновения или бесконтрольного пребывания в них посторонних лиц, а также просмотра посторонними лицами информации ограниченного доступа.

5.7 Режим охраны спецпомещений, в том числе порядок допуска работников в рабочее и нерабочее время, устанавливает руководитель Учреждения.

5.8 Двери спецпомещений должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода работников.

5.9 Для предотвращения просмотра извне окна спецпомещений должны быть защищены (шторы, жалюзи, светоотражающая пленка и т.д.).

5.10 Администратор безопасности для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих криптосредства носителей, должен иметь необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и приспособлениями для опечатывания.

5.11 При утрате ключа от хранилища или от входной двери в спецпомещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с оформлением акта. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает руководитель Учреждения.

5.12 При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно доложено администратору безопасности или руководителю. Администратор безопасности должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий и замене скомпрометированных криптоключей.

5.13 В спецпомещениях пользователей криптосредств и владельцев ключей шифрования для хранения выданных им ключевых документов, необходимо иметь надежно запираемые

шкафы (ящики, хранилища) индивидуального пользования, оборудованные приспособлениями для опечатывания.

5.14 При утрате ключа от замка хранилища или от входной двери в помещение пользователя криптосредства замок или секрет замка необходимо заменить.

5.15 Опечатанные хранилища пользователей криптосредств могут быть вскрыты только самими пользователями. В исключительных случаях разрешается вскрытие специально назначенной комиссией с разрешения руководителя Учреждения.

6. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

6.1 Лица, виновные в нарушении правил пользования криптосредствами, могут быть привлечены к административной или дисциплинарной ответственности.

6.2 Лица, виновные в нарушении безопасности информации ИСПДн, несут ответственность в соответствии с действующим законодательством Российской Федерации.

ПРИЛОЖЕНИЕ 1

Журнал поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов

Левая сторона

№ п/п	Наименование СКЗИ	Регистрационный номер СКЗИ	Номер экземпляра	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя СКЗИ	Дата и подпись получателя
1	2	3	4	5	6	7	8

Правая сторона

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

ПРИЛОЖЕНИЕ 2

Журнал учета пользователей криптосредств

№	Ф.И.О.	Должность	Данные о подготовке	Примечание
1	2	3	4	5

Примечание:

1. Журнал ведется по разделам для каждого криптосредства.

2. В графе 4 указывается номер и дата заключения по результатам обучения и допуска пользователя к самостоятельной работе с конкретным типом криптосредства.

3. В графе 5, в случае прекращения работы пользователя с криптосредством, производится соответствующая отметка.

4. Графу 3 допускается заполнять карандашом для возможности корректировки записей в случае перевода пользователя на другую должность, при условии, что он продолжает работать с криптосредством данного типа.

ПРИЛОЖЕНИЕ 3

УТВЕРЖДАЮ

_____
(руководитель)

«____» _____ 20__ г.

АКТ № ___
УСТАНОВКИ И ВВОДА В ЭКСПЛУАТАЦИЮ КРИПТОСРЕДСТВ

г. Белгород «____» _____ 20__ г.

Мы, нижеподписавшиеся, _____
(должность, Ф.И.О. пользователя и администратора безопасности)

_____

составили настоящий Акт о том, что на основании приказа (заявки, служебной записки)

_____ в помещении № ____ на ПЭВМ _____,
(№, дата документа) (№ системного блока)

находящейся в пользовании _____
(Ф.И.О. пользователя)

1. Установлены:
1.1. Средство криптографической защиты информации
_____
(название криптосредства, версия, сборка, серийный номер)

1.2. Настройки программного обеспечения по безопасности применения криптосредства в соответствии с правилами пользования и правами пользователя.
1.3. Дополнительное программное обеспечение:
_____

2. Переданы _____
(ключи, номера ключей, инструкция пользователя, памятки и т.п.)
_____

3. Проведена проверка целостности программного обеспечения и работоспособности криптосредства. Установленное ПО функционирует в штатном режиме.
4. Проведено обучение с принятием зачета _____
(Ф.И.О. пользователя)
по правилам пользования, соблюдению требований безопасности при работе с криптосредствами и выполнению правил обращения с ключевыми носителями, а также об ответственности за их нарушение.
5. Помещение № ____ и его оборудование, размещение ПЭВМ с установленным программным (программно-аппаратным) криптосредством, хранилища ключевых документов, охрана помещения и подготовленность пользователя к самостоятельной эксплуатации СКЗИ соответствует требования «Инструкции по криптографической защите информации».
6. Документы и программно-аппаратный комплекс _____
(тип и наименование криптосредства)
опечатанный печатью _____, приняты _____. Замечаний нет.
(№ печати) (Ф.И.О. пользователя)

_____ / _____ _____ / _____
(подпись и Ф.И.О. администратора безопасности) (подпись и Ф.И.О. пользователя)

«____» _____ 20__ г. «____» _____ 20__ г.

ПРИЛОЖЕНИЕ 4

РАЗРЕШАЮ

_____
(руководитель)

«____» _____ 20__ г.

ЗАЯВКА
НА ОБУЧЕНИЕ РАБОТЕ И УСТАНОВКУ КРИПТОСРЕДСТВА

Прошу Вас организовать подготовку к самостоятельной работе с криптографическим средством защиты информации _____ работника
(тип криптосредства)

_____
(Ф.И.О. и должность)

с установкой (без установки) криптосредства на его рабочее место.

Необходимость установки криптосредства обусловлена _____
(наименование решаемой задачи)

_____

_____

Администратор безопасности _____ / _____
(подпись) (Ф.И.О)

«____» _____ 20__ г.

ПРИЛОЖЕНИЕ 5

УТВЕРЖДАЮ

_____
(руководитель)

«____» _____ 20__ г.

ЗАКЛЮЧЕНИЕ
О ПОДГОТОВКЕ И ДОПУСКЕ К САМОСТОЯТЕЛЬНОЙ РАБОТЕ СО СРЕДСТВАМИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

_____
(должность, Ф.И.О.)

_____
(основание для подготовки, номер и дата заявки на подготовку пользователя)

_____
(наименование криптосредств, по которым осуществлялась подготовка)

Подготовка начата _____ Подготовка окончена _____
(дата) (дата)

Заключение комиссии: _____
(степень усвоения материала)

_____
(результат выполнения контрольных работ, возможность допуска к самостоятельной работе с криптосредством)

С заключением ознакомлен(а)

_____ _____
(подпись обучавшегося) (Ф.И.О.)

Члены комиссии:

_____ _____
(подпись) (Ф.И.О.)

_____ _____
(подпись) (Ф.И.О.)

ПРИЛОЖЕНИЕ 6

Аппаратный журнал учета эксплуатации криптосредств

1 раздел

№ п/п	Дата	Тип криптосредства, версия ПО	Номер аппаратного средства, в которое установлено криптосредство	Используемые криптоключи			Номер стикера (пломбира, печати)	Дата установки и роспись	Отметка об уничтожении		Примечание
				Тип ключевого документа	Серийный номер и номер экземпляра ключевого документа	Номер ключевого носителя			Дата	Подпись	
1	2	3	4	5	6	7	8	9	10	11	12

2 раздел

Дата, время	Содержание настроек (выполненные работы)	Ф.И.О. лица, производившего настройки (работы)	Подпись	Примечание
1	2	3	4	5

ПРИЛОЖЕНИЕ 7

УТВЕРЖДАЮ

_____
(руководитель)

«____» _____ 20__ г.

АКТ № ___
ПРИЕМА-ПЕРЕДАЧИ КРИПТОСРЕДСТВ, ТЕХНИЧЕСКОЙ, ЭКСПЛУАТАЦИОННОЙ ДОКУМЕНТАЦИИ, ПРАВИЛ ПОЛЬЗОВАНИЯ, КЛЮЧЕВЫХ НОСИТЕЛЕЙ

г. Белгород «____» _____ 20__ г.

Комиссия в составе председателя _____,
(должность, Ф.И.О.)

членов комиссии: _____
(должность, Ф.И.О.)

на основании _____
(№ приказа, распоряжения, в связи с увольнением и т.п.)

произвела проверку наличия и передачу следующих программных, программно-аппаратных средств, ключевых документов и эксплуатационной документации:

1. Инсталляционные, лицензионные носители криптосредства, техническая, эксплуатационная документация, правила работы согласно Журналу поэкземплярного учета № _____, с уч. № _____ по уч. № _____ в количестве _____ наименований.
2. Криптосредства, согласно Журналу поэкземплярного учета № _____, с уч. № _____ по уч. № _____ в количестве _____ наименований.
3. Машинные носители с ключевой информацией согласно Журналу поэкземплярного учета № _____, с уч. № _____ по уч. № _____ в количестве _____ наименований.
4. _____
(другие передаваемые аппаратные, программные средства, журналы учета, документация и т.п.)
_____

Все перечисленные программные, программно-аппаратные средства, ключевые документы и эксплуатационная документация оказалась в наличии. На отсутствующие средства и документацию предъявлены оправдательные документы: акты, сопроводительные письма.

Председатель комиссии: _____ _____
(подпись) (Ф.И.О.)

Члены комиссии: _____ _____
(подпись) (Ф.И.О.)

_____ _____
(подпись) (Ф.И.О.)

Перечисленные программные, программно-аппаратные средства, ключевые документы и эксплуатационную документацию:

СДАЛ: ПРИНЯЛ;

_____ _____ _____ _____
(подпись) (Ф.И.О.) (подпись) (Ф.И.О.)

ПРИЛОЖЕНИЕ 8

РАЗРЕШАЮ УНИЧТОЖИТЬ

(руководитель)

«____» _____ 20__ г.

АКТ № ___
НА УНИЧТОЖЕНИЕ КРИПТОСРЕДСТВ

г. Белгород «____» _____ 20___ г.

Комиссия в составе _____,
(должность, Ф.И.О.)

на основании _____ подготовила к уничтожению
(основание для уничтожение)

_____
(наименование, тип криптосредств, их номера, номера серий, комплектов, экземпляров)

в количестве _____ экземпляров.
(цифрами и прописью)

Всего подлежит уничтожению _ наименований _____ экземпляров.
(цифрами и прописью) (цифрами и прописью)

Председатель комиссии: _____ _____
(подпись) (Ф.И.О.)

Члены комиссии: _____ _____
(подпись) (Ф.И.О.)

_____ _____
(подпись) (Ф.И.О.)

Перечисленные криптосредства (программное обеспечение криптосредств, ключевая информация, содержащаяся на магнитных носителях информации, аппаратные, программно-аппаратные криптосредства и т.д.) после утверждения акта полностью уничтожены путем _____
_____
(переформатирования, удаления ПО криптосредств, физического уничтожения носителей)

с использование программы _____ входящей в комплект криптосредства

«____» _____ 20__ г.

Председатель комиссии: _____ _____
(подпись) (Ф.И.О.)

Члены комиссии: _____ _____
(подпись) (Ф.И.О.)

_____ _____
(подпись) (Ф.И.О.)

Отметка об уничтожении криптосредств (программного обеспечения криптосредств, ключевой информации, содержащейся на магнитных носителях информации, аппаратных, программно-аппаратных криптосредств), перечисленных в акте, в журнале _____
_____
(наименование журнала учета, его номер)

произвел _____ «____» _____ 20__ г.
(подпись, Ф.И.О.)