ИНСТРУКЦИЯ
по обращению со средствами криптографической защиты информации
в МАДОУ ДС№4

1. Термины и определения

1.1. Исходная ключевая информация – совокупность данных, предназначенных для выработки по определенным правилам криптоключей.

1.2. Ключевая информация – специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока.

1.3. Ключевой блокнот – набор бумажных ключевых документов одного вида (таблиц, перфолент, перфокарт и т.п.), сброшюрованных и упакованных по установленным правилам.

1.4. Ключевой документ – физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию.

1.5. Ключевой носитель – физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации).

1.6. Компрометация криптоключа – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

1.7. Контролируемая зона – территория объекта, на которой исключено неконтролируемое пребывание лиц или транспортных средств.

1.8. Криптографический ключ (криптоключ) – совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе.

1.9. Пользователь СКЗИ – физическое лицо, непосредственно допущенное к работе со средствами криптографической защиты информации.

1.10. Режимные помещения – помещения, где установлены средства криптографической защиты информации или хранятся ключевые документы к ним.

1.11. Средство криптографической защиты информации – криптосредства, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну.

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).

2. Общие положения

2.1. Настоящая Инструкция по обращению со средствами криптографической защиты информации в МАДОУ ДС№4 (далее – Инструкция), определяет порядок обращения, размещения, хранения, учета и уничтожения, сертифицированных ФСБ России шифровальных (криптографических) средств защиты информации (далее – СКЗИ), а также ответственных за эксплуатацию СКЗИ.

2.2. Инструкция разработана в соответствии со следующими документами:

- «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», утвержденное приказом ФСБ России № 66 от 9 февраля 2005 г.;
- Приказ ФАПСИ при Президенте РФ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
- Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

2.3. Требования настоящей Инструкции являются обязательными для исполнения всеми работниками МАДОУ ДС №4 (далее – Учреждение), использующими в своей работе СКЗИ.

2.4. Все работники Учреждения, использующие СКЗИ (далее –Пользователи СКЗИ), должны быть ознакомлены с требованиями настоящей Инструкцией под подпись.

2.5. Настоящая Инструкция является дополнением к действующим локальным нормативным актам (внутренним документам) по вопросам обеспечения безопасности сведений конфиденциального характера, в том числе и персональных данных, и не исключает обязательного выполнения их требований.

2.6. По всем вопросам организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ сведений конфиденциального характера Учреждение обязано обращаться к организации-лицензиату ФСБ России и выполнять его требования.

3. Ответственные лица

3.1. В Учреждении ответственность за эксплуатацию сертифицированных СКЗИ, несут:

а) Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных (далее – Ответственный за обеспечение безопасности ПДн в ИСПДн), на которого возлагаются обязанности по:

- выполнению мероприятий по обеспечению функционирования и безопасности, применяемых СКЗИ в соответствии с условиями выданных на них сертификатов, а также в соответствии с эксплуатационной и технической документацией к этим средствам;
- обучении лиц, использующих СКЗИ, правилам работы с СКЗИ и выдаче «Заключения о подготовке и допуске к самостоятельной работе со средствами криптографической защиты информации» по результатам прохождения обучения;
- поэкземплярному учету СКЗИ, эксплуатационной и технической документации к ним;
- учету лиц, допущенных к работе с СКЗИ;
- контролю за соблюдением условий использования и хранения СКЗИ в соответствии с эксплуатационной и технической документацией на СКЗИ и настоящей Инструкцией;
- расследованию и составлению заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации и разработке, и принятию мер по предотвращению возможных негативных последствий подобных нарушений.

б) Пользователи СКЗИ, на которых возлагаются обязанности по:

- обеспечению сохранности СКЗИ и ключевых документов, переданных им;
- соблюдению условий использования и хранения СКЗИ в соответствии с эксплуатационной и технической документацией на СКЗИ и настоящей Инструкцией.

4. Организация допуска пользователей к работе с СКЗИ

4.1. Обучение пользователей правилам работы с СКЗИ осуществляет Ответственный за обеспечение безопасности ПДн в ИСПДн. Непосредственно к работе с СКЗИ пользователи допускаются после обучения и выдачи «Заключения о подготовке и допуске к самостоятельной работе со средствами криптографической защиты информации», форма которого приведена в Приложении 1 к настоящей Инструкции.

5. Учет СКЗИ

5.1. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат учету с использованием индексов или условных наименований и регистрационных номеров в «Журнале поэкземплярного учета средств криптографической защиты информации, используемых в МАДОУ ДС№4, эксплуатационной и технической документации к ним, ключевых документов» (далее – Журнал учета СКЗИ), форма которого приведена в Приложении 2 к настоящей Инструкции.

5.2. Программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование.

5.3. 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.

5.4. Все полученные экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под подпись в Журнале учета СКЗИ Пользователям СКЗИ, несущим персональную ответственность за их сохранность.

5.5. При необходимости Пользователю СКЗИ выдается документация по эксплуатации СКЗИ с последующим возвратом Ответственному за обеспечение безопасности ПДн в ИСПДн.

5.6. Если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в СКЗИ, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в «Техническом (аппаратном) журнале учета средств криптографической защиты информации», форма которого приведена в Приложении 3 к настоящей Инструкции, ведущемся непосредственно Пользователем СКЗИ. В техническом (аппаратном) журнале СКЗИ отражают также данные об эксплуатации СКЗИ и другие сведения, предусмотренные эксплуатационной и технической документацией. В иных случаях технический (аппаратный) журнал на СКЗИ не заводится (если нет прямых указаний о его ведении в эксплуатационной или технической документации к СКЗИ).

5.7. Ответственный за обеспечение безопасности ПДн в ИСПДн заводит и ведет на каждого Пользователя СКЗИ лицевой счет, в котором регистрирует числящиеся за ними СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы. Форма лицевого счета пользователя СКЗИ приведена в Приложении 4 к настоящей Инструкции.

6. Хранение СКЗИ

6.1. Пользователи СКЗИ должны хранить инсталлирующие СКЗИ носители, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в шкафах (ящиках, хранилищах) в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

6.2. Пользователи СКЗИ должны предусмотреть раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов.

6.3. Для хранения ключевых документов, эксплуатационной и технической документации, дистрибутивов СКЗИ должно быть предусмотрено необходимое число шкафов (ящиков, 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 работника, ответственного за хранилище. Дубликаты ключей от хранилищ Пользователи СКЗИ хранят в сейфе Ответственного за обеспечение безопасности ПДн в ИСПДн под подпись в «Журнале учета ключей от режимных помещений, карт для доступа в режимные помещения, хранилищ, личных печатей от хранилищ», форма которого приведена в Приложении 5 к настоящей Инструкции.

6.4. Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы).

6.5. Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

7. Передача и выдача СКЗИ

7.1. При необходимости передачи по техническим средствам связи сведений конфиденциального характера, касающихся организации и обеспечения функционирования СКЗИ, указанные сообщения необходимо передавать только с использованием СКЗИ.

7.2. Передача криптоключей по техническим средствам связи не допускается, за исключением специально организованных систем с децентрализованным снабжением криптоключами.

7.3. Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между Пользователями СКЗИ и (или) Ответственным за обеспечение безопасности ПДн в ИСПДн под подпись в соответствующих Журналах учета СКЗИ. Такая передача между Пользователями СКЗИ должна быть санкционирована Ответственным за обеспечение безопасности ПДн в ИСПДн.

7.4. Выдача ключевых носителей, ключевых документов, СКЗИ, эксплуатационных и технических документов к СКЗИ Пользователям СКЗИ осуществляется Ответственным за обеспечение безопасности ПДн в ИСПДн на основании Журнала учета СКЗИ.

7.5. Факт выдачи пользователю ключевого документа, СКЗИ, эксплуатационного и технического документа к СКЗИ регистрируется в Журнала учета СКЗИ.

8. Пересылка и получение СКЗИ

8.1. СКЗИ и ключевые документы могут доставляться фельдъегерской (в том числе ведомственной) связью или со специально выделенными работниками Учреждения из числа Пользователей СКЗИ или Ответственного за обеспечение безопасности ПДн в

ИСПДн при соблюдении мер, исключающих бесконтрольный доступ к СКЗИ и ключевым документам во время доставки.

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

8.3. Для пересылки СКЗИ и ключевых документов они должны быть помещены в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия, в особенности на записанную ключевую информацию. СКЗИ пересылают отдельно от ключевых документов к ним. На упаковках указывают Пользователя СКЗИ, для которого 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.

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

8.5. Полученные упаковки вскрывает только Пользователь СКЗИ, для которого 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 СКЗИ и ключевые документы до получения указаний от отправителя применять не разрешается.

8.6. 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.

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

8.8. 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 за обеспечение безопасности ПДн в ИСПДн только после поступления от всех заинтересованных Пользователей СКЗИ подтверждения о получении ими очередных ключевых документов.

8.9. Неиспользованные или выведенные из действия ключевые документы подлежат возвращению Ответственному за обеспечение безопасности ПДн в ИСПДн или по его указанию должны быть уничтожены на месте.

9. Уничтожение СКЗИ

9.1. 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).

9.2. Криптоключи (исходную ключевую информацию) стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт-дисков (CD-ROM), Data Key, Smart Card, Touch Memory и т.п.). Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

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

9.4. Бумажные и прочие сгораемые ключевые носители, а также эксплуатационную и техническую документацию к СКЗИ уничтожают путем сжигания или с помощью любых бумагорезательных машин.

9.5. СКЗИ уничтожают (утилизируют) по решению Директора Учреждения, владеющего СКЗИ, и с уведомлением организации, ответственной в соответствии с Положением ПКЗ-2005 за организацию поэкземплярного учета СКЗИ.

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

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

9.8. Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. Если срок уничтожения эксплуатационной и технической документацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в Журнале учета СКЗИ. В эти же сроки с отметкой в техническом (аппаратном) журнале подлежат уничтожению разовые ключевые носители и ранее введенная, и хранящаяся в СКЗИ или иных дополнительных устройствах ключевая информация, соответствующая выведенным из действия

криптоключам, хранящиеся в криптографически защищенном виде данные следует перешифровать на новых криптоключах.

9.9. Разовые ключевые носители, а также электронные записи ключевой информации, соответствующей выведенным из действия криптоключам, непосредственно в СКЗИ или иных дополнительных устройствах уничтожаются Пользователями СКЗИ самостоятельно под подпись в техническом (аппаратном) журнале.

9.10. Ключевые документы уничтожаются либо Пользователями СКЗИ, либо Ответственным за обеспечение безопасности ПДн в ИСПДн под подпись в Журнале учета СКЗИ, а уничтожение большого объема ключевых документов может быть оформлено «Актом уничтожения шифровальных (криптографических) средств», форма которого приведена в Приложении 6 к настоящей Инструкции. При этом Пользователям СКЗИ разрешается уничтожать только использованные непосредственно ими (предназначенные для них) СКЗИ. После уничтожения Пользователи СКЗИ должны уведомить об этом письменно или устно Ответственного за обеспечение безопасности ПДн в ИСПДн.

9.11. Уничтожение по акту производит комиссия в составе не менее двух человек из числа Пользователей СКЗИ. 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, дистрибутивов СКЗИ, 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 Журнале учета СКЗИ.

10. Компрометация действующих ключей к СКЗИ

10.1. К событиям, связанным с компрометацией ключей, относятся, включая, но не ограничиваясь, следующие:

- явная компрометация ключей:
  - потеря ключевых носителей;
  - потеря ключевых носителей с их последующим обнаружением;
  - увольнение работников, имевших доступ к ключевой информации;
  - нарушение правил хранения и уничтожения (после окончания срока действия) закрытого ключа;
- неявная компрометация ключей:
  - возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
  - нарушение печати на сейфе с ключевыми носителями;
  - 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).

10.2. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшихся (хранящихся) с их использованием сведений конфиденциального характера, Пользователи СКЗИ обязаны сообщать Ответственному за обеспечение безопасности ПДн в ИСПДн.

11. Инструкция по восстановлению связи в случае компрометации действующих ключей к СКЗИ

11.1. Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия.

11.2. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается по решению Ответственного за обеспечение безопасности ПДн в ИСПДн, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а защищаемая информация как можно менее ценной.

11.3. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной информации, Пользователи СКЗИ обязаны сообщать Ответственному за обеспечение безопасности ПДн в ИСПДн.

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

11.5. В случаях недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

11.6. Мероприятия по розыску и локализации последствий компрометации ключевых документов организует и осуществляет Ответственный за обеспечение безопасности ПДн в ИСПДн.

11.7. Порядок оповещения Пользователей СКЗИ о предполагаемой компрометации криптоключей и их замене устанавливается Ответственным за обеспечение безопасности ПДн в ИСПДн или ФСБ России.

12. Режимные помещения

12.1. Размещение, специальное оборудование, охрана и организация режима в режимных помещениях (далее – РП) должны обеспечивать сохранность СКЗИ и ключевых документов к ним. При оборудовании РП должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ.

12.2. Перечень РП, выделенных для установки СКЗИ и хранения ключевых документов к ним утверждается приказом Директора Учреждения.

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

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

12.5. Режим охраны РП, в том числе правила допуска работников и посетителей в рабочее и нерабочее время, устанавливает Ответственный за обеспечение безопасности ПДн в ИСПДн по согласованию с Директором Учреждения. Установленный режим охраны

должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются.

12.6. Двери РП должны быть постоянно закрыты на замок и могут открываться только для санкционированного прохода работников и посетителей. Ключи от входных дверей нумеруют, учитывают и выдают работникам, имеющим право допуска в РП, под подпись в «Журнале учета ключей от режимных помещений, карт для доступа в режимные помещения, хранилищ, личных печатей от хранилищ». Дубликаты ключей от входных дверей таких РП следует хранить в сейфе Ответственного за обеспечение безопасности ПДн в ИСПДн.

12.7. Дубликат ключа от сейфа Ответственного за обеспечение безопасности ПДн в ИСПДн в опечатанной упаковке должен быть передан на хранение Директору Учреждения под подпись в «Журнале учета ключей от режимных помещений, карт для доступа в режимные помещения, хранилищ, личных печатей от хранилищ».

12.8. Для предотвращения просмотра извне РП их окна должны быть защищены ставнями, жалюзи, шторами и т.п.

12.9. РП по возможности должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации. Исправность сигнализации периодически необходимо проверять совместно с представителем службы охраны или дежурным по организации с отметкой в соответствующих журналах.

12.10. По окончании рабочего дня РП и установленные в нем хранилища должны быть закрыты, хранилища опечатаны. Находящиеся в пользовании ключи от хранилищ должны быть сданы под подпись в соответствующем журнале уполномоченному (дежурному), которые хранят эти ключи в личном или специально выделенном хранилище.

12.11. Ключи от РП в опечатанном виде должны быть сданы под подпись в соответствующем журнале службы охраны или дежурному по организации одновременно с передачей под охрану самих РП. Печати, предназначенные для опечатывания хранилищ, должны находиться у Пользователей СКЗИ, ответственных за эти хранилища.

12.12. При утрате ключа от хранилища или от входной двери в РП 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 обеспечение безопасности ПДн в ИСПДн.

12.13. В обычных условиях РП, находящиеся в них опечатанные хранилища, могут быть вскрыты только Пользователями СКЗИ или Ответственным за обеспечение безопасности ПДн в ИСПДн.

12.14. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти РП или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено Ответственному за обеспечение безопасности ПДн в ИСПДн, который должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять при необходимости меры к локализации последствий компрометации информации и к замене скомпрометированных криптоключей.

12.15. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в РП должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое

обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ.

12.16. На время отсутствия Пользователей СКЗИ указанное оборудование при наличии технической возможности должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с Ответственным за обеспечение безопасности ПДн в ИСПДн необходимо предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами.

13. Регламент проведения контроля соответствия использования СКЗИ

13.1. Контроль за организацией и обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ сведений конфиденциального характера в Учреждении осуществляют уполномоченные федеральные органы исполнительной власти или организация-лицензиат. В ходе контроля изучаются и оцениваются:

- организация безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации конфиденциального характера;
- достигнутый уровень криптографической защиты информации конфиденциального характера;
- условия использования СКЗИ.

13.2. По результатам государственного контроля составляется подробный или краткий акт, справка. С актом проверки (справкой) под подпись должен быть ознакомлен Директор Учреждения.

13.3. Если в использовании СКЗИ обнаружены недостатки, то Ответственный за обеспечение безопасности ПДн в ИСПДн обязан принять безотлагательные меры по их устранению.

13.4. Ответственный за обеспечение безопасности ПДн в ИСПДн обязан контролировать выполнение Пользователями СКЗИ требований по организации и обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ сведений конфиденциального характера, а также условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ, сертификатом ФСБ России и Инструкцией.

13.5. Внутренний контроль за организацией и обеспечением безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ сведений конфиденциального характера производится в Учреждении 1 раз в год.

13.6. В ходе контроля изучаются и оцениваются:

- организация безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ сведений конфиденциального характера;
- выполнение Инструкции.

13.7. С целью оценки обоснованности и достаточности мер, принятых для защиты информации конфиденциального характера, Учреждение вправе обратиться в ФСБ России с просьбой о проведении контроля за соблюдением правил пользования СКЗИ и условий их использования, указанных в правилах пользования СКЗИ.

14. Ответственность

14.1. Пользователи СКЗИ и Ответственный за обеспечение безопасности ПДн в ИСПДн несут личную ответственность за сохранность выданной им ключевой информации, носителей и паролей доступа к ним.

14.2. Пользователи СКЗИ, осуществляющие обработку и защиту персональных данных на, обязаны ознакомиться с данной Инструкцией под подпись.

14.3. Пользователи СКЗИ и Ответственный за обеспечение безопасности ПДн в ИСПДн несут персональную ответственность за выполнение требований настоящей Инструкции.

15. Срок действия и порядок внесения изменений

15.1. Настоящая Инструкция вступает в силу с момента её утверждения и действует бессрочно.

15.2. Настоящая Инструкция подлежит пересмотру не реже одного раза в три года.

15.3. Изменения и дополнения в настоящую Инструкцию вносятся приказом Директора Учреждения.

Приложение 2
к Инструкции по обращению с
шифровальными (криптографическими)
средствами защиты информации в
МАДОУ ДС№4

ФОРМА

Журнал поэкземплярного учета средств криптографической защиты информации используемых в МАДОУ ДС№4, эксплуатационной и технической документации к ним, ключевых документов

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные 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 СКЗИ	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 СКЗИ, производившего 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. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

Приложение 3
к Инструкции по обращению с
шифровальными (криптографическими)
средствами защиты информации в
МАДОУ ДС№4

ФОРМА

Технический (аппаратный) журнал
учета средств криптографической защиты информации

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

Приложение 4
к Инструкции по обращению с
шифровальными (криптографическими)
средствами защиты информации в
МАДОУ ДС№4

ФОРМА

Лицевой счет пользователя СКЗИ

№ п/п	Наименование СКЗИ, 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	Номер и дата сопроводительного документа при получении	Номер и дата сопроводительного документа при передаче	Ответственный исполнитель	Примечание
1	2	3	4	5	6	7	8

Приложение 5
к Инструкции по обращению с
шифровальными (криптографическими)
средствами защиты информации в
МАДОУ ДС№4

ФОРМА

Журнал учета ключей от режимных помещений, карт для доступа в режимные помещения, ключей хранилищ, личных печатей от хранилищ

№ п/п	Наименование объекта учета (ключ от помещения/ключ от хранилища/личная печать/карта)	№ помещения/ № хранилища	Информация о выдаче	Информация о получении	Информация о сдаче	Примечание
			Фамилия И.О., подпись, дата	Фамилия И.О., подпись, дата	Фамилия И.О., подпись, дата	
1	2	3	4	5	6	7

Приложение 2
к приказу МАДОУ ДС№4
от «___» _____ 2023 г. № _____

ПЕРЕЧЕНЬ
режимных помещений МАДОУ ДС№4, выделенных для установки средств криптографической защиты информации и хранения ключевых документов к ним

№ п/п	Наименование/ номер помещения	Адрес расположения помещения	Допущенные работники (Фамилия И.О., должность)	Ответственный за режим в помещении (Фамилия И.О., должность)
1				
2				
3				

Приложение 3
к приказу МАДОУ ДС№4
от «___» _____ 2023 г. № _____

ПЕРЕЧЕНЬ
защищенных хранилищ, предназначенных для хранения средств криптографической защиты информации, ключевых документов, эксплуатационной и технической документации к средствам криптографической защиты информации

№ п/п	Номер хранилища	Номер помещения, где расположено хранилище	Адрес расположения помещения	Ответственный за хранилище (Фамилия И.О., должность)
1.				
2.				
3.				

Приложение 4
к приказу МАДОУ ДС№4
от «___» _____ 2023 г. № _____

ПЕРЕЧЕНЬ
работников, допущенных к работе с шифровальными (криптографическими) средствами защиты информации

№ п/п	Должность	Фамилия И.О.	Основание допуска к криптосредству	Наименование криптосредства
1.			Заключение о подготовке и допуске к самостоятельной работе со средствами криптографической защиты информации	
2.			Заключение о подготовке и допуске к самостоятельной работе со средствами криптографической защиты информации	
3.			Заключение о подготовке и допуске к самостоятельной работе со средствами криптографической защиты информации	