

ПРИЛОЖЕНИЕ №1

УТВЕРЖДЕНО

Приказом

МДОБУ «Кудровский ДСКВ №4»

«Об утверждении организационно-распорядительных
документов в области использования средств криптографической защиты информации»

Заведующий

Михайлова Марина Тайфиковна

(подпись, печать)

«24» февраля 2025 г.

ПОЛОЖЕНИЕ

**по использованию средств криптографической защиты информации в МДОБУ
«Кудровский ДСКВ №4»**

Оглавление

1. Общие положения	3
2. Порядок применения криптосредств.....	7
3. Обязанности ответственного пользователя криптосредств	9
4. Обязанности пользователей криптосредств	12
5. Пользователям криптосредств запрещается	13
6. Порядок учета криптосредств, эксплуатационной и технической документации к криптосредствам, ключевых документов действия при компрометации.....	14
7. Порядок уничтожения криптосредств.....	16
8. Охрана, специальное оборудование и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним	18
9. Порядок доступа к хранилищам криптосредств	19
10. Ответственность пользователей криптосредств	20
Приложение № 1	21
Приложение № 2	23
Приложение № 3	24
Приложение № 4	25
Приложение № 5	28
Приложение № 6	29
Приложение № 7	31
Приложение № 8	34

1. Общие положения

1.1. Настоящее Положение по использованию средств криптографической защиты информации (далее - Положение) определяет в МДОБУ «Кудровский ДСКВ №4» порядок обращения со средствами криптографической защиты информации (криптосредствами).

1.2. Сокращения, термины и определения:

В настоящем Положении используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
ИСПДн	Информационная система персональных данных
СКЗИ, криптосредство	Средство криптографической защиты информации
ФАПСИ	Федеральное агентство правительственной связи и информации при Президенте Российской Федерации
ФСБ России	Федеральная служба безопасности Российской Федерации
ФЗ от 06.04.2011 №63-ФЗ	Федеральный закон от 06.04.2011 №63-ФЗ «Об электронной подписи»
Приказ ФАПСИ от 13.06.2001 № 152	Приказ Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации»

Сокращение	Расшифровка сокращения
Приказ ФСБ России от 09.02.2005 № 66 (Положение ПКЗ-2005)	приказ Федеральной службы безопасности Российской Федерации от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение ПКЗ-2005)»

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Информация	Сведения (сообщения, данные) независимо от формы их представления	ГОСТ Р 50922-2006
Информационная система	Совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	ГОСТ Р 51583-2014
Ключевая информация	Специальным образом организованная совокупность криптоключей, предназначенных для осуществления криптографической защиты информации в течение определенного срока	Приказ ФАПСИ от 13.06.2001 № 152
Ключевой документ	Физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости – контрольную, служебную и технологическую информацию	Приказ ФАПСИ от 13.06.2001 № 152
Компрометация криптоключей	Хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате	Приказ ФАПСИ от 13.06.2001 № 152

Термин	Определение	Источник
	которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам	
Контролируемая зона	Пространство, в пределах которого осуществляется контроль над пребыванием и действиями лиц и/или транспортных средств	ГОСТ Р 56115-2014
Криптографический ключ (криптоключ)	Совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе	Приказ ФАПСИ от 13.06.2001 № 152
Пользователь СКЗИ	Физическое лицо, непосредственное допущенное к работе с СКЗИ	Приказ ФАПСИ от 13.06.2001 № 152
Спецпомещение	Помещение, где установлены СКЗИ или хранятся ключевые документы к ним	Приказ ФАПСИ от 13.06.2001 № 152
СКЗИ	Шифровальные (криптографические) средства защиты информации конфиденциального характера К СКЗИ относятся: - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, обеспечивающие безопасность информации при ее обработке, хранении и передаче по каналам связи, включая СКЗИ;	Приказ ФАПСИ от 13.06.2001 № 152

Термин	Определение	Источник
	- реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от несанкционированного доступа к информации при ее обработке и хранении; - реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и "электронной подписи"; - аппаратные, программные и аппаратно-программные средства, системы и комплексы изготовления и распределения ключевых документов для СКЗИ независимо от вида носителя ключевой информации.	

1.3. Перечень нормативных правовых актов, на основании которых разработано настоящее Положение:

- приказ Федерального агентства правительственной связи и информации при президенте РФ от 13.06.2001 № 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 Федеральной службы безопасности Российской Федерации от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение ПКЗ-2005)»;

- приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378 «Об утверждении Состав 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 требованиям к защите персональных данных для каждого из уровней защищенности».

2. Порядок применения криптосредств

2.1. Для обеспечения безопасности персональных данных при их обработке в ИСПДн должны использоваться сертифицированные в системе сертификации ФСБ России криптосредства.

Класс криптосредства определяется в соответствии с приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состав 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».

2.2. Ответственность за эксплуатацию средств криптографической защиты информации в ИСПДн возлагается на ответственного пользователя криптосредств.

2.3. Ответственный пользователь криптосредств назначается приказом Заведующий МДОБУ «Кудровский ДСКВ №4»

При смене ответственного пользователя криптосредств должны быть внесены изменения в приказ МДОБУ «Кудровский ДСКВ №4»

«О назначении ответственного пользователя средств криптографической защиты информации в МДОБУ «Кудровский ДСКВ №4».

2.4. Ответственный пользователь криптосредств должен быть ознакомлен с настоящим документом, Инструкцией ответственного пользователя средств

криптографической защиты информации, Инструкцией пользователя средств криптографической защиты информации и нормативными правовыми актами Российской Федерации, регламентирующими обеспечение безопасности информации с использованием криптосредств.

По результатам ознакомления осуществляется соответствующая запись в Журнале ознакомления работников с нормативными правовыми актами Российской Федерации и локальными актами МДОБУ «Кудровский ДСКВ №4» по обеспечению безопасности информации с использованием криптосредств (Приложение №1).

2.5. Основанием для предоставления доступа к работе с криптосредствами является внесение работника в Перечень лиц, допущенных к работе со средствами криптографической защиты информации в МДОБУ «Кудровский ДСКВ №4», утверждаемый приказом Заведующий МДОБУ «Кудровский ДСКВ №4».

2.6. Пользователи криптосредств допускаются к работе с криптосредствами после прохождения обучения правилам работы с СКЗИ и ознакомления с настоящим Положением, Инструкцией пользователя криптосредств и нормативными правовыми актами Российской Федерации, регламентирующими обеспечение безопасности информации с использованием криптосредств.

По результатам прохождения обучения правилам работы с криптосредствами оформляется Заключение о подготовке и допуске к самостоятельной работе со средствами криптографической защиты информации (Приложение №2). По результатам ознакомления работников осуществляется соответствующая запись в Журнале ознакомления работников с нормативными правовыми актами Российской Федерации и локальными актами МДОБУ «Кудровский ДСКВ №4» по обеспечению безопасности информации с использованием криптосредств.

2.7. При наличии двух и более пользователей криптосредств обязанности между ними должны быть распределены с учетом персональной ответственности за сохранность криптосредств, ключевой, эксплуатационной и технической документации, а также за порученные участки работы.

2.8. Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в спецпомещениях пользователей криптосредств должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам.

2.9. Системные блоки технических средств (или иные аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, аппаратные и аппаратно-программные СКЗИ) с установленными СКЗИ должны оборудоваться средствами контроля за их вскрытием (опечатываться, опломбироваться). Место опечатывания (опломбирования) системного блока должно быть таким, чтобы его можно было визуально контролировать.

2.10. Техническое обслуживание криптосредств, а также другого оборудования, функционирующего с криптосредствами, смена криптоключей осуществляются в отсутствии лиц, не допущенных к работе с данными криптосредствами.

2.11. Криптосредства, а также другое оборудование, функционирующее с криптосредствами, на время отсутствия пользователей, при наличии такой технической возможности, выключается, отключается от линии связи и убирается в опечатываемые хранилища. В противном случае предусматриваются организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

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

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

3. Обязанности ответственного пользователя криптосредств

3.1. Ответственный пользователь криптосредств обязан:

- проводить обучение пользователей криптосредств правилам работы с криптосредствами с оформлением Заключения о подготовке и допуске к самостоятельной работе со средствами криптографической защиты информации и отметкой в Журнале ознакомления работников с нормативными правовыми актами Российской Федерации и локальными актами МДОБУ «Кудровский ДСКВ №4» по обеспечению безопасности защищаемой информации с использованием криптосредств;

- вести поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним, ключевых документов с документальным оформлением в

Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов по установленной форме (Приложение № 4);

- контролировать заполнение Акта установки и ввода в эксплуатацию средств криптографической защиты информации (Приложение №3), делать отметку Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

- хранить Акты установки и ввода в эксплуатацию средств криптографической защиты информации;

- организовать надежное хранение установочных комплектов СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, носителей конфиденциальной информации, ключей от металлических хранилищ (сейфов);

- вести учет лиц, допущенных к работе с СКЗИ. Формировать и актуализировать приказом МДОБУ «Кудровский ДСКВ №4» Перечень лиц, допущенных к работе со средствами криптографической защиты информации в МДОБУ «Кудровский ДСКВ №4»;

- заводить и вести лицевые счета на каждого пользователя СКЗИ, в котором регистрировать числящиеся за ним СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы (Приложение №5);

- вести учет металлических хранилищ (сейфов), предназначенных для хранения устанавливающих СКЗИ носителей, эксплуатационной и технической документации к криптосредствам, ключевых документов с документальным оформлением в Журнале учета металлических хранилищ (сейфов) (Приложение №6);

- проводить не реже одного раза в год проверку создаваемой приказом МДОБУ «Кудровский ДСКВ №4» комиссии соблюдения условий использования криптосредств с оформлением акта проверки соблюдения использования средств криптографической защиты информации (Приложение 7);

- осуществлять контроль за ведением пользователем криптосредства технического (аппаратного) журнала (Приложение №8) в случае, 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;

- проводить периодический контроль за состоянием технических средств охраны (при их наличии) совместно с представителем службы охраны или дежурным по организации с отметкой в Журнале контроля состояния охранной сигнализации;
- осуществлять контроль за проведением работ по размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ в спецпомещениях пользователей СКЗИ;
- контролировать целостность печатей (пломб) на технических средствах с установленными СКЗИ пользователей криптосредств;
- контролировать наличие и актуальность Перечня помещений, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информацией СКЗИ, утвержденного приказом МДОБУ «Кудровский ДСКВ №4»;
- контролировать наличие и актуальность Перечня лиц, имеющих право доступа в Помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информацией СКЗИ, утвержденного приказом МДОБУ «Кудровский ДСКВ №4»;
- соблюдать режим конфиденциальности информации, которая стала известной в процессе выполнения должностных (трудовых) обязанностей, в том числе сведений о криптоключях, паролях и применяемых СКЗИ, организации хранения, обработки и передачи связи информации с использованием СКЗИ;
- выполнять требования эксплуатационных и регламентирующих документов по обеспечению безопасности защищаемой информации, обрабатываемых в ИС с использованием СКЗИ;
- немедленно уведомлять руководителя МДОБУ «Кудровский ДСКВ №4» о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах компрометации криптоключей, которые могут привести к разглашению информации ограниченного доступа, а также о причинах и условиях возможной утечки такой информации;
- организовывать мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, передаваемой (хранящейся) с использованием СКЗИ.

4. Обязанности пользователей криптосредств

4.1. Пользователь криптосредств обязан:

- получить у Ответственного пользователя криптосредства СКЗИ, эксплуатационную и техническую документацию, ключевые документы с документальным оформлением (под расписку в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов);
- получить у Ответственного пользователя криптосредств ключ от металлического хранилища (сейфа) для хранения устанавлирующих СКЗИ носителей, эксплуатационной и технической документации к криптосредствам, ключевых документов с документальным оформлением (под расписку в Журнале учета металлических хранилищ (сейфов);
- хранить устанавливающие СКЗИ носители, эксплуатационную и техническую документацию к СКЗИ, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение. Хранить резервные ключевые документы, предназначенные для применения в случае компрометации действующих криптоключей, отдельно от действующих ключевых документов;
- вести технический (аппаратный) журнал в случае, 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. Регистрировать в техническом (аппаратном) журнале разовый ключевой носитель или электронную запись соответствующего криптоключа, а также отражать данные об эксплуатации СКЗИ и другие сведения, предусмотренные эксплуатационной и технической документацией. Самостоятельно уничтожать разовые ключевые носители, электронные записи ключевой информации, соответствующей выведенным из действия криптоключам, и делать об этом отметку под расписку в техническом (аппаратном) журнале;
- выполнять требования эксплуатационных и регламентирующих документов по обеспечению безопасности защищаемой информации, обрабатываемой в ИСПДн с использованием СКЗИ;

- контролировать целостность печатей (пломб) на системных блоках технических средствах с установленными СКЗИ;
- осуществлять уничтожение ключевых документов с документальным оформлением (под расписку в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов) после окончания срока действия, не позднее 10 суток после вывода их из действия, если иной срок уничтожения не предусмотрен эксплуатационной и технической документацией к СКЗИ;
- сообщать Ответственному пользователю криптосредств и непосредственному руководителю структурного подразделения МДОБУ «Кудровский ДСКВ №4» о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
- немедленно уведомлять Ответственного пользователя криптосредств и руководителя организации МДОБУ «Кудровский ДСКВ №4» о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений;
- немедленно выводить из действия криптоключи, в отношении которых возникло подозрение в компрометации, с уведомлением Ответственного пользователя криптосредств и руководителя организации МДОБУ «Кудровский ДСКВ №4» с последующим их уничтожением.

5. Пользователям криптосредств запрещается

- разглашать информацию о ключевых документах и информацию ограниченного доступа;
- вносить любые изменения в программное обеспечение СКЗИ, изменять настройки СКЗИ;
- допускать к использованию СКЗИ посторонних лиц;
- осуществлять вскрытие системных блоков технических средств с установленными СКЗИ, подключать к ним дополнительные устройства;
- использовать криптоключи, в отношении которых возникло подозрение в компрометации;

- оставлять ключевые носители без контроля, выносить их за пределы служебных помещений;
- снимать копии с ключевых документов;
- записывать на ключевой носитель информацию, не предусмотренную правилами пользования СКЗИ (служебные файлы, текстовые и мультимедийные файлы и т.п.);
- допускать установку ключевых документов в другие ПЭВМ;
- выводить ключевую информацию на средствах отображения информации (дисплей монитора, печатающие устройства, проекторы и т.п.).

6. Порядок учета криптосредств, эксплуатационной и технической документации к криптосредствам, ключевых документов действия при компрометации

6.1. Используемые или хранимые СКЗИ, эксплуатационная и техническая документации к ним, ключевые документы подлежат поэкземплярому учету в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Заполнение, ведение и хранение Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов осуществляет ответственный пользователь криптосредств.

6.2. Пользователям криптосредств выдаются все экземпляры ключевых документов, СКЗИ, эксплуатационная и техническая документация к криптосредствам под расписку в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов. В случае увольнения или отстранении от исполнения обязанностей, связанных с использованием СКЗИ, пользователи криптосредств обязаны сдать все экземпляры ключевых документов, криптосредства, эксплуатационную и техническую документацию к ним под расписку в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов Ответственному пользователю криптосредств.

6.3. Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов между пользователями криптосредств запрещена.

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

6.5. Программные СКЗИ учитываются совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются с соответствующими аппаратными средствами.

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

6.7. 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 регистрируются в техническом (аппаратном) журнале, ведущемся непосредственно пользователем СКЗИ. В техническом (аппаратном) журнале отражают также данные об эксплуатации СКЗИ и другие сведения, предусмотренные эксплуатационной и технической документацией. В иных случаях технический (аппаратный) журнал на СКЗИ не заводится (если нет прямых указаний о его ведении в эксплуатационной или технической документации к СКЗИ).

6.8. Не реже одного раза в год осуществляется проверка создаваемой приказом МДОБУ «Кудровский ДСКВ №4» комиссией (в состав комиссии включается Ответственный за организацию обработки персональных данных, Ответственный пользователь криптосредств), соблюдения условий использования криптосредств с оформлением акта проверки соблюдения использования средств криптографической защиты информации.

6.9. Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи немедленно выводятся из действия, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам.

7. Порядок уничтожения криптосредств

7.1. 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).

7.2. Криптоключи (исходную ключевую информацию) стираются по технологии, принятой для соответствующих ключевых носителей многократного использования. 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).

7.3. Ключевые носители уничтожаются 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).

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

7.5. СКЗИ уничтожаются (утилизируются) на основании приказа МДОБУ «Кудровский ДСКВ №4».

7.6. Подлежащие к уничтожению (утилизации) СКЗИ подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом СКЗИ считаются изъятими из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СКЗИ процедура удаления программного обеспечения СКЗИ и они полностью отсоединены от аппаратных средств. В Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов проставляется отметка об изъятии СКЗИ из аппаратных средств.

7.7. 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).

7.8. 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 поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов. 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 криптоключях.

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

7.10. Ключевые документы уничтожаются пользователями СКЗИ под расписку в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов. При этом пользователям СКЗИ разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи.

8. Охрана, специальное оборудование и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним

8.1. Охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним (далее – спецпомещения), должны обеспечивать сохранность информации, криптосредств и ключевых документов к ним, исключать возможность неконтролируемого проникновения или пребывания в помещениях посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

8.2. Спецпомещения выделяются с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к СКЗИ.

8.3. Спецпомещения оборудуются прочными входными дверями с замками, гарантирующими надежное закрытие спецпомещений в нерабочее время. Двери спецпомещений должны быть постоянно закрыты на замок и открываться только для санкционированного прохода, оборудованы приспособлениями для опечатывания или техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

8.4. Окна спецпомещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, оснащаются металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения. Для предотвращения просмотра извне спецпомещений окна должны быть защищены.

8.5. По окончании рабочего дня спецпомещения должны быть закрыты, опечатаны. Ключи от спецпомещений нумеруют, учитывают и выдают работникам, имеющим право допуска в помещение. Дубликаты ключей от входных дверей спецпомещений хранятся в опечатанной упаковке в сейфе Ответственного пользователя криптосредств.

8.6 Периодический контроль за состоянием технических средств охраны (при их наличии) проводится Ответственным пользователем криптосредств совместно с представителем службы охраны или дежурным по организации с отметкой в Журнале контроля состояния охранной сигнализации.

8.7. Режим охраны помещений в том числе правила допуска работников и посетителей в рабочее и нерабочее время, определен в документации о внутрипропускном и объектовом режимах, установленной приказом МДОБУ «Кудровский ДСКВ №4».

9. Порядок доступа к хранилищам криптосредств

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

9.2. Металлические хранилища (сейфы), предназначенные для хранения устанавливающих СКЗИ носителей, эксплуатационной и технической документации к криптосредствам, ключевых документов (далее – хранилища) должны быть оборудованы внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин.

9.3. Должно быть предусмотрено раздельное безопасное хранение пользователями криптосредств действующих и резервных ключевых документов, предназначенных для применения, в случае компрометации действующих ключевых документов.

9.4. Все ключи от механических замков хранилищ нумеруются и учитываются Ответственным пользователем криптосредств в Журнале учета металлических хранилищ (сейфов).

9.5. Рабочий ключ от хранилища предоставляется работнику, ответственному за данное хранилище, с документальным оформлением (под расписку в Журнале учета металлических хранилищ (сейфов)).

9.6. Дубликаты ключей от хранилищ в опечатанной упаковке хранятся в сейфе Ответственного пользователя криптосредств. Дубликаты ключей от хранилища Ответственного пользователя криптосредств передаются на хранение руководителю МДОБУ «Кудровский ДСКВ №4» под расписку в Журнале учета металлических хранилищ (сейфов).

9.7. При необходимости доступа к содержимому хранилища работник, ответственный за данное хранилище, проверяет его целостность, открывает

механический замок с использованием ключа, а по окончании рабочего дня закрывает и опечатывает хранилище, за которое он ответственен.

9.8. Печати, предназначенные для опечатывания хранилищ, должны находиться у работников, ответственных за данные е хранилища.

9.9. При утрате ключа от хранилища пользователь криптосредства немедленно уведомляет Ответственного пользователя криптосредств и непосредственного руководителя структурного подразделения МДОБУ «Кудровский ДСКВ №4».

9.10. Замок от данного хранилища 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 документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает ответственный пользователь криптосредств.

9.11. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в хранилище посторонних лиц, о случившемся немедленно сообщается Ответственному пользователю криптосредств и руководителю МДОБУ «Кудровский ДСКВ №4». Ответственный пользователь криптосредств должен оценить возможность компрометации, хищения, подмены, порчи хранящихся документов и технических средств, составить акт и принять, при необходимости, меры к локализации последствий.

10. Ответственность пользователей криптосредств

Ответственный пользователь криптосредств и пользователи криптосредств несут ответственность за несоблюдение требований документов, регламентирующих организацию и обеспечение функционирования и безопасности СКЗИ, предназначенных для защиты конфиденциальной информации, в соответствии с действующим законодательством Российской Федерации.

Приложение № 1
к Положению по использованию средств
криптографической защиты информации
в МДОБУ «Кудровский ДСКВ №4»

Журнал
ознакомления работников с нормативными правовыми актами Российской Федерации
и локальными актами МДОБУ «Кудровский ДСКВ №4»
по обеспечению безопасности информации с использованием криптосредств

Журнал начат _____

Журнал окончен _____

Листов (_____)

[illegible]

Приложение № 2
к Положению по использованию средств
криптографической защиты информации в МДОБУ
«Кудровский ДСКВ №4»

Заключение

о подготовке и допуске к самостоятельной работе со средствами криптографической
защиты информации

(должность, Фамилия, имя, отчество работника)

(основание для подготовки)

(наименование криптосредства)

Подготовка начата _____, окончена _____

Подготовка проводилась в соответствии с требованиями
эксплуатационной и технической документации к криптосредству

Заключение:

Допустить пользователя к самостоятельной работе со средствами криптографической
защиты информации

(наименование криптосредства)

С заключением ознакомлен (а)

(подпись обучавшегося)

(Фамилия, Инициалы)

Ответственный пользователь криптосредств:

(подпись)

(Фамилия, Инициалы)

« ____ » _____ 20 __ г

Г. _____

М.П.

Приложение № 4
к Положению по использованию средств
криптографической защиты информации
в МДОБУ «Кудровский ДСКВ №4»

Журнал
поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов
МДОБУ «Кудровский ДСКВ №4»

Журнал начат _____

Журнал окончен _____

Листов (_____) _____

[illegible]

[illegible]

Пользователь _____

[illegible]

Приложение № 6
к Положению по использованию средств
криптографической защиты информации
в МДОБУ «Кудровский ДСКВ №4»

Журнал
учета металлических хранилищ (сейфов)
МДОБУ «Кудровский ДСКВ №4»

Журнал начат _____

Журнал окончен _____

Листов (_____) _____

Тип хранилища _____
(сейф, металлический шкаф)

Заводской номер _____

Инвентарный номер _____

Количество ключей и их номера _____

[illegible]

Приложение № 7
к Положению по использованию средств
криптографической защиты информации в МДОБУ
«Кудровский ДСКВ №4»

Акт № _____
проверки соблюдения условий использования
средств криптографической защиты информации

Г. _____

«_____» _____ Г.

Комиссия в составе:

Председатель комиссии: _____

(должность. ФИО)

Члены комиссии: _____

(должность. ФИО)

(должность. ФИО)

на основании произвела проверку

(приказ о назначении комиссии)

соблюдения условий использования криптосредств в МДОБУ «Кудровский ДСКВ №4» в соответствии с требованиями «Положения по использованию средств криптографической защиты информации».

В ходе работы комиссии установлено:

1. Инсталлирующие СКЗИ носители, эксплуатационная и техническая документация к ним в электронном виде и на бумажных носителях согласно Журналу поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (Учетные номера)

в наличии;

_____ (оказались/не оказались)

2. Криптосредства, установленные на технические средства пользователей согласно Журналу поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (Учетные номера) в наличии;

_____ (оказались/ не оказались)

3. Ключевые документы пользователей криптосредств согласно Журналу поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (Учетные номера _____) _____ в наличии;
(оказались/не оказались)

4. Лицевые счета пользователей криптосредств находятся в _____ состоянии;
(актуальном /неактуальном)

5. Перечень лиц, допущенных к работе со средствами криптографической защиты информации в МДОБУ «Кудровский ДСКВ №4» утвержден приказом руководителя МДОБУ «Кудровский ДСКВ №4» от _____ № _____ и находится в _____ состоянии;
(актуальном /неактуальном)

6. Перечень Помещений, в которых размещены используемые СКЗИ, хранятся СКЗИ (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, в МДОБУ «Кудровский ДСКВ №4» утвержден приказом руководителя МДОБУ «Кудровский ДСКВ №4» _____ от _____ № _____ и находится в _____ состоянии;
(актуальном/неактуальном)

7. В Помещениях, в которых размещены используемые СКЗИ, хранятся СКЗИ (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, требования по обеспечению режима, препятствующего возможности неконтролируемого проникновения или пребывания в них _____ ;

(выполняются/не выполняются)

Режим хранения устанавливающих СКЗИ носителей, эксплуатационной и технической документацию к криптосредствам, ключевых документов в металлических хранилищах (сейфах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, их непреднамеренное уничтожение _____ ;

(соблюдается /не соблюдается)

8. Металлические хранилища (сейфы) пользователей криптосредств и ключи от них согласно Журналу учета металлических хранилищ (сейфов) (Учетные номера _____) _____ в наличии;
(оказались/не оказались)

9. Техническое состояние СКЗИ и оборудование, функционирующее с СКЗИ требованиям эксплуатационной документации на СКЗИ, информационную систему и систему защиты информации _____ ;
(соответствует/ не соответствует)

10. Пользователи криптосредств с нормативными правовыми актами Российской Федерации и локальными актами МДОБУ «Кудровский ДСКВ №4»

_____;
(ознакомлены/ не ознакомлены)

11. Пользователями криптосредств требования правил хранения, использования и защиты СКЗИ _____;
(выполняются / не выполняются)

12. Случаи компрометации СКЗИ _____.
(установлены/ не установлены)

Действия по устранению причин и локализации последствий компрометации СКЗИ:
_____ (в случае установления фактов компрометации СКЗИ)

В ходе работы комиссии выявлены следующие недостатки:

Заключение комиссии:

Соблюдение условий использования средств криптографической защиты информации _____ требованиям к условиям использования СКЗИ в МДОБУ «Кудровский ДСКВ №4».
(соответствует/ не соответствует)

Председатель комиссии:

_____ (должность) _____ (подпись) _____ (ФИО)

Члены комиссии:

_____ (должность) _____ (подпись) _____ (ФИО)

_____ (должность) _____ (подпись) _____ (ФИО)

Приложение № 8
к Положению по использованию средств
криптографической защиты информации
в МДОБУ «Кудровский ДСКВ №4»

Технический (аппаратный) журнал

Журнал начат _____

Журнал окончен _____

Листов (_____) _____

[illegible]