МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ГОРОДА НЕФТЕЮГАНСКА «ДЕТСКИЙ САД № 9 «РАДУГА»

МАДОУ "ДЕТСКИЙ САД № 9 "РАДУГА"

Подписано цифровой подписью: МАДОУ "ДЕТСКИЙ САД № 9 "РАДУГА"

ПРИКАЗ

13.02.2024 **№ 99**

Об организации криптографической защиты информации

В целях исполнения Приказа ФСБ России от 10.07.2014 № 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», приказа ФАПСИ 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"

ПРИКАЗЫВАЮ:

1. Назначить ответственным пользователем средств криптографической защиты информации (СКЗИ) в муниципальном автономном дошкольном образовательном учреждении города Нефтеюганска «Детский сад № 9 «Радуга» (далее-МАДОУ «Детский сад № 9 «Радуга») специалиста по кадрам Винокурову А.П..
2. Утвердить перечень пользователей СКЗИ Муниципального автономного дошкольного образовательного учреждения города Нефтеюганска «Детский сад № 9 «Радуга» (Приложение № 1).
3. Утвердить инструкцию пользователя средств криптографической защиты информации (Приложение № 2).
4. Утвердить инструкцию по организации и обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах (Приложение № 3).
5. Допустить к работе с СКЗИ вышеуказанных пользователей после

изучения руководящих документов по использованию СКЗИ, инструкции пользователя СКЗИ и обучения работе с СКЗИ.

6. Утвердить форму журнала поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов (Приложение № 4).

7. Считать утратившим силу приказ муниципального автономного дошкольного образовательного учреждения города Нефтеюганска «Детский сад № 9 «Радуга» от 09.01.2023 № 59 «Об организации криптографической защиты информации».

8. Контроль за исполнением настоящего приказа оставляю за собой.

Директор Ю.А. Ячникова

Приложение № 1
к приказу от 13.02.2024 № 99

ПЕРЕЧЕНЬ
пользователей средств криптографической защиты информации Муниципального автономного дошкольного образовательного учреждения города Нефтеюганска «Детский сад № 9 «Радуга»:

№ п/п	Фамилия, имя, отчество	Занимаемая должность
1.		директор
2.		главный бухгалтер
3.		бухгалтер
4.		бухгалтер
5.		специалист по кадрам
6.		делопроизводитель
7.		юрисконсульт

Приложение № 2
к приказу от 13.02.2024 № 99

ИНСТРУКЦИЯ
пользователя средств криптографической защиты информации

1. Общие положения

1.1. Настоящая Инструкция пользователя средств криптографической защиты информации (СКЗИ) (далее – Инструкция) Муниципального автономного дошкольного образовательного учреждения города Нефтеюганска «Детский сад № 9 «Радуга» (далее - МАДОУ «Детский сад № 9 «Радуга») определяет права и обязанности пользователей СКЗИ, порядок обращения с СКЗИ, а также определяет порядок восстановления связи в случае компрометации действующих ключей к СКЗИ.

1.2. Пользователем СКЗИ является сотрудник МАДОУ «Детский сад № 9 «Радуга», включенный в список сотрудников, допущенных к работе с СКЗИ, предназначенными для обеспечения безопасности персональных данных, обрабатываемых в информационных системах персональных данных МАДОУ «Детский сад № 9 «Радуга», утвержденный директоромМАДОУ «Детский сад № 9 «Радуга».

1.3. Пользователь СКЗИ должен знать законодательные и иные нормативные правовые акты Российской Федерации в сфере обработки персональных данных, а также в области защиты информации при ее передаче по открытым каналам связи с использованием СКЗИ.

1.4. В своей деятельности, связанной с обработкой персональных данных с использованием СКЗИ, пользователь СКЗИ руководствуется настоящей Инструкцией.

1.5. Пользователи СКЗИ несут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту СКЗИ от несанкционированного использования.

2. Обязанности и права пользователя СКЗИ

2.1. Пользователь СКЗИ обязан:

– соблюдать требования по обеспечению безопасности функционирования СКЗИ;

– обеспечить конфиденциальность всей информации ограниченного распространения, доступной по роду выполняемых функциональных обязанностей;

– сдать ответственному Пользователю СКЗИ МАДОУ «Детский сад № 9 «Радуга» носители ключевой информации (далее – НКИ) при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

– сдать ответственному Пользователю СКЗИ НКИ по окончании срока действия сертификата ключа, а также в случае компрометации ключа;

– немедленно уведомлять ответственного Пользователя СКЗИ о компрометации НКИ, о фактах утраты или недостачи СКЗИ;

– в пределах своей компетенции предоставлять информацию комиссии, проводящей служебные расследования по фактам компрометации, а также выявлению причин нарушения требований безопасности функционирования СКЗИ.

2.2. Пользователю СКЗИ запрещается:

– осуществлять несанкционированное и безучётное копирование ключевых данных;

– хранить НКИ вне сейфов и помещений, гарантирующих их сохранность и конфиденциальность;

– передавать НКИ кому-либо, кроме ответственного Пользователя СКЗИ;

– во время работы оставлять НКИ без присмотра (например, на рабочем столе или в разъеме системного блока ПЭВМ);

– хранить на НКИ какую-либо информацию, кроме ключевой;

– использовать в помещениях, где применяются СКЗИ, личные технические средства, позволяющие осуществлять копирование ключевой информации;

– использовать НКИ, выведенные из действия.

2.3. Пользователь имеет право:

– вносить предложения ответственному Пользователю СКЗИ по вопросам использования СКЗИ;

– повышать уровень квалификации по использованию СКЗИ.

3. Порядок обращения с СКЗИ

3.1. Служебные помещения, в которых размещаются СКЗИ, должны отвечать всем требованиям по оборудованию и охране, предъявляемым к помещениям, выделенным для работы с конфиденциальной информацией. Для хранения НКИ помещения обеспечиваются сейфами (металлическими шкафами), оборудуются охранной сигнализацией и по убытии сотрудников закрываются, опечатываются личными печатями ответственных лиц (либо закрываются кодовым замком) и сдаются под охрану.

3.2. Для хранения НКИ пользователь СКЗИ должен быть обеспечен личным сейфом. В случае отсутствия индивидуального сейфа по окончании рабочего дня пользователь СКЗИ обязан сдавать НКИ ответственному Пользователю СКЗИ.

3.3. Дубликаты ключей от сейфов (а также значения кодов – при наличии кодовых замков) пользователей СКЗИ должны храниться в сейфе руководителя структурного подразделения или ответственного Пользователя СКЗИ в упаковках, опечатанных личными печатями пользователей СКЗИ. Несанкционированное изготовление дубликатов ключей запрещено. В случае утери ключа механизм (секрет) замка (либо сам сейф) должен быть заменён.

3.4. К эксплуатации СКЗИ допускаются лица, прошедшие соответствующую подготовку и изучившие правила пользования данным СКЗИ.

3.5. Все программное обеспечение ПЭВМ, предназначенной для установки СКЗИ, должно иметь соответствующие лицензии. Установка средств разработки и отладки программ на рабочую станцию, использующую СКЗИ, не допускается.

4. Восстановление связи в случае компрометации действующих ключей к СКЗИ

4.1. Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию владельца НКИ и конфиденциальность информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих криптографических ключей, относятся:

– утрата (хищение) НКИ, в том числе – с последующим их обнаружением;

– увольнение (переназначение) сотрудников, имевших доступ к НКИ;

– передача секретных ключей по линии связи в открытом виде;

– нарушение правил хранения НКИ;

– вскрытие фактов утечки передаваемой информации или её искажения (подмены, подделки);

– ошибки при совершении криптографических операций;

– несанкционированное или безучётное копирование ключевой информации;

– все случаи, когда нельзя достоверно установить, что произошло с НКИ (в том числе случаи, когда НКИ вышел из строя и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий).

4.2. При наступлении любого из перечисленных выше событий пользователь СКЗИ или владелец НКИ должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) ответственному Пользователю СКЗИ лично, по телефону, электронной почте или другим доступным способом. В любом случае пользователь СКЗИ или владелец НКИ обязан убедиться, что его сообщение получено и прочтено.

4.3. При подтверждении факта компрометации действующих ключей пользователь СКЗИ обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей и сдачу ответственному Пользователю СКЗИ в течении 3-х рабочих дней.

4.4. Для восстановления конфиденциальной связи после компрометации действующих ключей пользователь СКЗИ получает у ответственного Пользователя СКЗИ новые ключи.

к приказу от 13.02.2024 № 99

ИНСТРУКЦИЯ
по организации и обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах

1. Термины и определения

В настоящей Инструкции по организации и обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах (далее – Инструкция) применяются следующие термины и определения:

Доступ к информации - возможность получения информации и ее использования.

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

Информация ограниченного доступа - информация, доступ к которой ограничен федеральными законами.

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

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

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

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

Ключевой носитель - физический носитель определенной структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации). Различают разовый ключевой носитель (таблица, перфолента, перфокарта и т.п.) и ключевой носитель многократного использования (магнитная лента, дискета, компакт - диск, Data Key, Smart Card, Touch Memory и т.п.).

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

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

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя

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

Лицензиат ФСБ – оператор конфиденциальной связи и лица, имеющие лицензию ФСБ и не являющиеся операторами конфиденциальной связи.

Орган криптографической защиты – организация, структурное подразделение организации - лицензиата ФСБ, обладателя конфиденциальной информации или физическое лицо.

Пользователи СКЗИ – физические лица, непосредственно допущенные к работе с СКЗИ.

Средства криптографической защиты информации (СКЗИ) – сертифицированные ФСБ (ФАПСИ) России средства:

- 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;
- 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.

Специализированные помещения - помещения, где установлены СКЗИ или хранятся ключевые документы к ним.

2. Общие положения

2.1. Настоящий документ определяет порядок учета, хранения и использования СКЗИ и криптографических ключей, в целях обеспечения безопасности эксплуатации СКЗИ в Муниципальном автономном дошкольном образовательном учреждении города Нефтеюганска «Детский сад № 9 «Радуга» (далее – Учреждение).

2.2. Настоящая Инструкция разработана в соответствии с:

- Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом ФСБ России от 9 февраля 2005 г. № 66;

- Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной Приказом ФАПСИ от 13 июня 2001 г. № 152;
- Составом и содержанием 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, утвержденными Приказом ФСБ России от 10 июля 2014 г. № 378.

2.3. Для организации и обеспечения работ по техническому обслуживанию СКЗИ и управления криптографическими ключами приказом директора Учреждения назначается Ответственный пользователь СКЗИ, выполняющий функции органа криптографической защиты информации и имеющий необходимый уровень квалификации.

Ответственный пользователь СЗКИ осуществляет:

- поэкземплярный учет СКЗИ;
- контроль за соблюдением условий использования СКЗИ, установленных эксплуатационной и технической документацией на СКЗИ и настоящей Инструкцией;
- расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации.

2.4. Список Пользователей СКЗИ утверждается приказом директора Учреждения.

2.5. Пользователь СКЗИ обязан:

- строго соблюдать правила пользования СКЗИ и требования настоящей Инструкции;
- не допускать установки на ПЭВМ нештатных программ, предупреждать возможность занесения вирусов и других вредоносных программ;
- не разглашать информацию, к которой они допущены, в том числе сведения о СКЗИ, ключевых документах к ним и других мерах защиты;
- соблюдать требования к обеспечению безопасности информации ограниченного доступа, требования к обеспечению безопасности СКЗИ и ключевых документов к ним;
- сообщать о ставших ему известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
- немедленно уведомлять Ответственного пользователя СЗКИ 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 защищаемой информации;

- сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с установленным порядком при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
- не допускать снятие копий с ключевых документов;
- не допускать вывод ключевых документов на дисплей (монитор) ПЭВМ или принтер;
- не допускать записи на ключевой носитель посторонней информации;
- не допускать установки ключевых документов в другие ПЭВМ.

2.6. Непосредственно к работе с СКЗИ Пользователи допускаются только после соответствующего обучения. Обучение пользователей правилам работы с СКЗИ осуществляет Ответственный пользователь СЗКИ.

2.7. Текущий контроль, обеспечение функционирования и безопасности СКЗИ возлагается на Ответственного пользователя СЗКИ.

2.8. Ответственный пользователь СЗКИ и Пользователи СКЗИ должны быть ознакомлены с положениями настоящей Инструкцией под расписку.

3. Учет, хранение СКЗИ и криптографических ключей

3.1. Учет криптографических средств

3.1.1. Криптосредства, эксплуатационная и техническая документация к ним, используемые для обеспечения безопасности информации ограниченного доступа, подлежат учету с использованием индексов или условных наименований и регистрационных номеров.

3.1.2. Все поступившие СКЗИ, эксплуатационная и техническая документации к ним, а также ключевые документы должны быть взяты на поэкземплярный учет и внесены в «Журнал поэкземплярного учета криптосредств эксплуатационной и технической документации к ним, ключевых документов» (далее – журнал поэкземплярного учета). При этом программные криптосредства должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные криптосредства подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие криптосредства учитываются также совместно с соответствующими аппаратными средствами.

3.1.3. Поэкземплярный учет СКЗИ имеет цель обеспечить контроль за снабжением СКЗИ, их наличием, движением, расходованием и исключить обезличенное пользование ими. В журнале поэкземплярного учета должно отражаться полное прохождение каждого в отдельности экземпляра СКЗИ, эксплуатационной и технической документации к ним, ключевых документов с момента получения до уничтожения.

3.1.4. Единицей поэкземплярного учета криптографических средств, ключевых документов считается ключевой носитель многократного использования, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

3.1.5. Журнал поэкземплярного учета ведет Ответственный пользователь СКЗИ.

3.1.6. Все полученные экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов выдаются под расписку в соответствующем журнале поэкземплярного учета Пользователям СКЗИ, несущим персональную ответственность за их сохранность.

3.1.7. При увольнении, перемещении Пользователя СКЗИ все числящие за ним СКЗИ и другие документы передаются по акту (Приложение № 1) сотруднику, которому поручено исполнять его обязанности. При временном убытии сотрудника (в том числе командировку, отпуск, по болезни) по акту могут быть переданы только СКЗИ и документы, необходимые для работы в период его отсутствия. Остальные числящие СКЗИ и документы должны находиться в хранилище (упаковке), опечатанном его личной печатью. Акты составляются в одном экземпляре.

3.2. Хранение криптографических средств

3.2.1. Незадействованные в эксплуатации СКЗИ, дистрибутивы СКЗИ на магнитных носителях, эксплуатационная и техническая документация к ним хранится у Ответственного пользователя СКЗИ. Криптографические ключи хранятся у Пользователей СКЗИ.

3.2.2. Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-програмные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать.

3.2.3. Инсталлирующие СКЗИ носители, эксплуатационная и техническая документация к СКЗИ, ключевые документы хранятся в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

3.2.4. Действующие и резервные ключевые документы, предназначенные для применения в случае компрометации действующих криптоключей, хранятся раздельно.

3.3. Рассылка СКЗИ, ключевых документов

3.3.1. Криптосредства и ключевые документы могут доставляться фельдъегерской (в том числе ведомственной) связью или со специально выделенными нарочными, которыми могут быть Ответственный пользователь СКЗИ или Пользователи СКЗИ, при соблюдении мер, исключающих бесконтрольный доступ к криптосредствам и ключевым документам во время доставки. Эксплуатационную и техническую документацию к СКЗИ можно пересылать заказными или ценными почтовыми отправлениями.

3.3.2. Для пересылки СКЗИ, эксплуатационной и технической документации к ним, ключевых документов следует подготовить сопроводительное письмо (Приложение № 2), в котором необходимо указать, что посылается и в каком количестве, учетные номера изделий или документов, а также, при необходимости, назначение и порядок

использования высылаемого отправления. Сопроводительное письмо вкладывают в одну из упаковок.

3.3.3. Полученные упаковки вскрывают пользователи СКЗИ, для которых они предназначены. Если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или сама упаковка и печать - их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то получатель составляет акт, который высылает отправителю.

3.3.4. 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 изготовителя.

3.3.5. Получение СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должно быть подтверждено отправителю в соответствии с порядком, указанным в сопроводительном письме.

3.4. Уничтожение СКЗИ, ключевых документов

3.4.1. СКЗИ уничтожают (утилизируют) в соответствии с требованиями эксплуатационной и технической документации к ним.

3.4.2. 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.

3.4.3. 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).

3.4.4. СКЗИ, 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 соответствующих журналах поэкземплярного учета.

3.4.5. О проведенном уничтожении СКЗИ, эксплуатационной и технической документации к ним, ключевых документов, делаются отметки в соответствующих журналах учета.

3.4.6. Не реже одного раза в год пользователи СКЗИ должны направлять Ответственному пользователю СКЗИ письменные отчеты об уничтоженных ключевых документах.

3.5. Компрометация криптоключей

3.5.1. Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ. О выводе криптоключей из действия сообщают Ответственному пользователю СКЗИ. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается, по решению Ответственного пользователя СКЗИ, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а передаваемая информация как можно менее ценной.

3.5.2. О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием информации, Пользователи СКЗИ обязаны сообщать Ответственному пользователю СКЗИ. Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения). В случаях недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

3.5.3. Необходимо провести мероприятия по розыску и локализации последствий компрометации информации, передававшейся (хранящейся) с использованием СКЗИ.

4. Размещение, охрана и организация режима в помещениях, где установленны СКЗИ

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

4.2. При оборудовании специализированных помещений должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с криптосредствами.

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

охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

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

4.5. Режим охраны помещений, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает Ответственный пользователь СКЗИ по согласованию с директором Учреждения. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны. Внутриобъектовый режим устанавливается отдельной инструкцией.

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

4.7. Размещение и монтаж криптосредств, а также другого оборудования, функционирующего с криптосредствами, в специализированных помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

4.8. 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 пользователем СКЗИ необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

4.9. В специализированных помещениях Пользователей СКЗИ для хранения выданных им ключевых документов, эксплуатационной и технической документации, инсталлирующих СКЗИ носителей необходимо иметь достаточное число надежно запираемых шкафов (ящиков, хранилищ) индивидуального пользования, оборудованных приспособлениями для опечатывания замочных скважин. Ключи от этих хранилищ должны находиться у соответствующих Пользователей СКЗИ.

4.10. При утрате Пользователем СКЗИ ключа от хранилища или от входной двери в специализированное помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить.

4.11. В обычных условиях опечатанные хранилища Пользователей СКЗИ могут быть вскрыты только самими пользователями.

4.12. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в специализированные помещения или несанкционированное вскрытие хранилищ посторонними лицами, о случившемся должно быть немедленно сообщено директору и Ответственному пользователю СКЗИ. Ответственный пользователь СКЗИ

должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации информации ограниченного доступа и к замене скомпрометированных криптоключей.

Приложение № 4
к приказу от 13.02.2024 № 99

(ФОРМА)
ЖУРНАЛ
поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов

На ___ листах

Начат «__» _____ 201__ г. Окончен «__» _____ 201__ г.

Ответственный за журнал: _____ «__» _____ 201__ г.
Должность, ФИО, подпись

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийный номер СКЗИ эксплуатационной и технической документации к ним, ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке СКЗИ)			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
				От кого получены	Дата и номер сопроводительного письма	ФИО пользователя	Дата и расписка в получении	ФИО сотрудников органа криптографической защиты	Дата подключения (установки) и подписи лиц, производивших подключение	Номера аппаратных средств, в которые установлены СКЗИ	Дата изъятия (уничтожения)	ФИО сотрудников органа криптографической защиты	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15