

Муниципальное бюджетное  
дошкольное образовательное учреждение  
«Центр развития ребенка – детский сад № 58 «Жемчужинка»

ПРИКАЗ

29.11.16 № 134  
- об утверждении инструкции

П р и к а з ы в а ю:

Утвердить инструкцию по организации и обеспечению безопасности эксплуатации шифровальных (криптографических) средств в информационных системах.

Заведующий



Н.А. Алексеева

## Инструкция

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

#### 1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. В настоящей Инструкции 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 России.

**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 Государственном бюджетном учреждении «Учреждение» (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 от 13 июня 2001 г. №152;

- Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденными ФСБ России от 21 февраля 2008 г. № 149.

**2.3.** Для организации и обеспечения работ по техническому обслуживанию СКЗИ и управления криптографическими ключами назначается *Администратор безопасности*, имеющий необходимый уровень квалификации, назначаемый приказом руководства Учреждения (далее – АБ).

АБ 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. Пользователи СКЗИ** назначаются приказом руководства 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 им известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;
- немедленно уведомлять АБ 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 осуществляют сотрудники соответствующего органа криптографической защиты.

**2.7.** Текущий контроль, обеспечение функционирования и безопасности СКЗИ возлагается на АБ.

**2.8.** АБ и Пользователи СКЗИ должны быть ознакомлены с Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных,

утвержденными ФСБ России от 21 февраля 2008 г. № 149 и 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 документация к ним должны быть взяты на поэкземплярный учет по Журналу поэкземплярного учета криптографических средств, эксплуатационной и технической документации к ним. 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, расходом и исключить обезличенное пользование ими. В журнале поэкземплярного учета должно отражаться полное прохождение каждого в отдельности экземпляра СКЗИ, эксплуатационной и технической документации к ним 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 СКЗИ, эксплуатационной и технической документации к ним, ключевых документов ведет АБ.

**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.** Недействующие в эксплуатации СКЗИ, дистрибутивы СКЗИ на магнитных носителях, эксплуатационная и техническая документация к ним хранится у АБ. 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 отдельно.

### *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 ответственными Пользователями СКЗИ и сотрудниками 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 вернуть 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 изъятными 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 в орган криптографической защиты 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 в соответствующий орган криптографической защиты. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается, по решению органа криптографической защиты, 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 в соответствующий орган криптографической защиты. 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.

### **3.5.4. РАЗМЕЩЕНИЕ, ОХРАНА И ОРГАНИЗАЦИЯ РЕЖИМА В ПОМЕЩЕНИЯХ, ГДЕ УСТАНОВЛЕННЫ СКЗИ**

**3.6.** 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.

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

**3.8.** 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.

**3.9.** 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.

**3.10.** Режим охраны помещений, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает АБ по согласованию с руководством Учреждения. Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны. Внутриобъектовый режим устанавливается отдельной инструкцией.

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

**3.12.** 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.

**3.13.** 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 АБ необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

**3.14.** В специализированных помещениях пользователей СКЗИ для хранения выданных им ключевых документов, эксплуатационной и технической документации, устанавливающих 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.



**3.15.** При утрате ключа от хранилища или от входной двери в специализированное помещение пользователя СКЗИ 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.

**3.16.** В обычных условиях опечатанные хранилища пользователей СКЗИ могут быть вскрыты только самими пользователями.

**3.17.** При обнаружении признаков, указывающих на возможное несанкционированное проникновение в специализированное помещение или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено руководству Учреждения и руководителю органа криптографической защиты. Прибывшие сотрудники органа криптографической защиты должны 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.