УТВЕРЖДЕНО
приказом директора
Краевого государственного бюджетного учреждения
дополнительного профессионального образования
работников культуры
"Камчатский учебно-методический центр"
от 01.09.2015 г. № 63-а

ПОЛОЖЕНИЕ

о работе по организации обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием сертифицированных ФАПСИ средств криптографической защиты (шифровальных средств) подлежащей в соответствии с законодательством Российской Федерации обязательной защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в Краевом государственном бюджетном учреждении дополнительного профессионального образования работников культуры «Камчатский учебно–методический центр»

Петропавловск-Камчатский городской округ, 2015 г.

1.Общие положения

Положение о работе по организации обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием сертифицированных Федеральным агентством правительственной связи и информации при Президенте Российской Федерации **(**далее - ФАПСИ) средств криптографической защиты (шифровальных средств) подлежащей в соответствии с законодательством Российской Федерации обязательной защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну**,** (далее - Положение) КГБУ ДПО КУМЦ разработано в соответствии с 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. N 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"**.**

Настоящее Положение определяет единый на территории Российской Федерации порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием сертифицированных ФАПСИ средств криптографической защиты (шифровальных средств) подлежащей в соответствии с законодательством Российской Федерации обязательной защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну**.**

Настоящее Положение вступает в силу со дня его утверждения.

2. Понятия и определения

Конфиденциальная информация - информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну.

Сертифицированные ФАПСИ средства криптографической защиты конфиденциальной информации именуются – СКЗИ, 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;
- 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.

Обладателями конфиденциальной информации могут быть государственные органы, государственные организации и другие организации независимо от их организационно-правовой формы и формы собственности, индивидуальные предприниматели и физические лица.

Сети конфиденциальной связи - сети связи, предназначенные для передачи конфиденциальной информации.

Операторы конфиденциальной связи - операторы связи, предоставляющие на основании лицензии ФАПСИ услуги конфиденциальной связи с использованием СКЗИ.

Операторы конфиденциальной связи и лица, имеющие лицензию ФАПСИ и не являющиеся операторами конфиденциальной связи, в настоящей Инструкции именуются лицензиаты ФАПСИ.

Органом криптографической защиты может быть организация, структурное подразделение организации - лицензиата ФАПСИ, обладателя конфиденциальной информации. Функции органа криптографической защиты могут быть возложены на физическое лицо.

Физические лица, непосредственно допущенные к работе с СКЗИ, в настоящей Инструкции именуются - пользователи СКЗИ.

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

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

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

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.);

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

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

Помещения, где установлены СКЗИ или хранятся ключевые документы к ним, именуются - спецпомещения.

Требования к обеспечению сохранности конфиденциальной информации в спецпомещениях аналогичны требованиям к помещениям, где выполняются работы, связанные с хранением (обработкой) такой информации, и устанавливаются обладателем конфиденциальной информации;

Под федеральными органами правительственной связи и информации понимаются главные управления ФАПСИ, управления ФАПСИ в федеральных округах, региональные управления правительственной связи и информации, центры правительственной связи.

2. Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации

Безопасность хранения, обработки и передачи по **каналам связи** с использованием СКЗИ конфиденциальной информации в сетях конфиденциальной связи организуют и обеспечивают операторы конфиденциальной связи.

Безопасность хранения и обработки с использованием СКЗИ конфиденциальной информации, передаваемой **вне сетей** конфиденциальной связи, организуют и обеспечивают лица, имеющие лицензию ФАПСИ.

Безопасность хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации, обладатели которой не имеют лицензий ФАПСИ, лицензиаты ФАПСИ организуют и обеспечивают либо по указанию вышестоящей организации, либо на основании договоров на оказание услуг по криптографической защите

конфиденциальной информации.

Лицензиаты ФАПСИ обеспечивают и несут ответственность за комплексность защиты конфиденциальной информации, в том числе посредством применения некриптографических средств защиты.

Орган криптографической защиты осуществляет:

-проверку готовности обладателей конфиденциальной информации к самостоятельному использованию СКЗИ и составление заключений о возможности эксплуатации СКЗИ (с указанием типа и номеров используемых СКЗИ, номеров аппаратных, программных и аппаратно-программных средств, где установлены или к которым подключены СКЗИ, с указанием также номеров печатей (пломбиров), которыми опечатаны (опломбированы) технические средства, включая СКЗИ, и результатов проверки функционирования СКЗИ);

-разработку мероприятий по обеспечению функционирования и безопасности применяемых СКЗИ в соответствии с условиями выданных на них сертификатов, а также в соответствии с эксплуатационной и технической документацией к этим средствам;

-обучение лиц, использующих СКЗИ, правилам работы с ними;

-контроль за соблюдением условий использования СКЗИ, установленных эксплуатационной и технической документацией к СКЗИ, сертификатом ФАПСИ и настоящей Инструкцией;

-расследование и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению уровня защиты конфиденциальной информации; разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

КГБУ ДПО КУМЦ, как обладатель конфиденциальной информации, обязан выполнять указания по криптографической защите по всем вопросам организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации, в соответствии с Положением ПКЗ-99.

Для организации взаимодействия обладателей конфиденциальной информации, безопасности хранения, обработки и передачи по каналам связи которой с использованием СКЗИ организуют и обеспечивают различные лицензиаты ФАПСИ, из созданных этими лицензиатами ФАПСИ органов криптографической защиты выделяется координирующий орган криптографической защиты. Все органы криптографической защиты, образованные этими лицензиатами ФАПСИ, обязаны выполнять указания координирующего органа криптографической защиты по обеспечению такого взаимодействия.

10. Инструкции, регламентирующие процессы подготовки, ввода, обработки, хранения и передачи защищаемой с использованием СКЗИ конфиденциальной информации, подготавливаются согласно эксплуатационной и технической документации на соответствующие сети связи, автоматизированные и информационные системы, в которых передается, обрабатывается или хранится конфиденциальная информация, с учетом используемых СКЗИ и согласовывается с лицензиатом ФАПСИ.

К работе с СКЗИ допускаются работники КГБУ ДПО КУМЦ согласно перечню пользователей СКЗИ, утверждаемому директором КГБУ ДПО КУМЦ и только после соответствующего обучения.

Пользователи СКЗИ обязаны:

-не разглашать конфиденциальную информацию, к которой они допущены, рубежи ее защиты, в том числе сведения о **криптоключах**;

-соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;

-сообщать в орган криптографической защиты о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ или **ключевых документах** к ним;

-сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящей Инструкцией, при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

-немедленно уведомлять орган криптографической защиты 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.

3. Порядок обращения с СКЗИ и криптоключами к ним. Мероприятия при компрометации криптоключей

Предназначенные для обеспечения безопасности хранения, обработки и передачи по каналам связи конфиденциальной информации СКЗИ, а также **ключевые документы** к ним не должны содержать сведений, составляющих **государственную тайну**.

Для организации и обеспечения безопасности хранения, обработки и передачи по каналам связи конфиденциальной информации следует использовать СКЗИ, позволяющие реализовать принцип абонентского шифрования и предусматривающие запись криптоключей на электронные **ключевые носители** многократного (долговременного) использования (дискеты, компакт-диски (CD-ROM), Data Key, Smart Card, Touch Memory и т.п.).

При необходимости передачи по техническим средствам связи служебных сообщений, касающихся организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ конфиденциальной информации, соответствующие указания необходимо передавать, только применяя СКЗИ. Передача по техническим средствам связи криптоключей не допускается, за исключением специально организованных систем с децентрализованным снабжением криптоключами.

Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету по установленным формам в соответствии с требованиями **Положения ПКЗ-99**. При этом программные СКЗИ должны учитываться 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 также совместно с соответствующими аппаратными средствами.

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

Журналы поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов ведут как органы криптографической защиты, так и обладатели конфиденциальной информации.

Все полученные обладателем конфиденциальной информации 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.

Если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых **ключевых носителей** или **криптоключи** вводят и хранят (на весь срок их действия) непосредственно в СКЗИ, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в техническом (аппаратном) журнале, ведущемся непосредственно пользователем СКЗИ. В техническом (аппаратном) журнале отражают также данные об эксплуатации СКЗИ и другие сведения, предусмотренные эксплуатационной и технической документацией. Технический (аппаратный) журнал на СКЗИ не заводится, если нет прямых указаний о его ведении в эксплуатационной или технической документации к СКЗИ.

Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ и (или) сотрудниками органа криптографической защиты под расписку в соответствующих журналах поэкземплярного учета.

Пользователи СКЗИ хранят инсталлирующие 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.

Пользователи СКЗИ предусматривают также раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих криптоключей.

Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. При наличии технической возможности на время отсутствия пользователей СКЗИ указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

При обнаружении бракованных ключевых документов или **криптоключей** один экземпляр бракованного изделия следует возвратить изготовителю через соответствующий орган криптографической защиты для установления причин происшедшего и их устранения в дальнейшем, а оставшиеся экземпляры хранить до поступления дополнительных указаний от органа криптографической защиты или изготовителя.

Неиспользованные или выведенные из действия **ключевые документы** подлежат возвращению в орган криптографической защиты или по его указанию должны быть уничтожены на месте.

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).

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

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

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

СКЗИ уничтожают (утилизируют) в соответствии с требованиями **Положения ПКЗ-99** по решению обладателя конфиденциальной информации, владеющего СКЗИ, и по согласованию с лицензиатом ФАПСИ.

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.

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).

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. В эти же сроки с отметкой в техническом (аппаратном) журнале подлежат уничтожению разовые ключевые носители и ранее введенная и хранящаяся в СКЗИ или иных дополнительных устройствах **ключевая информация**, соответствующая выведенным из действия криптоключам; хранящиеся в криптографически защищенном виде данные следует перешифровать на новых **криптоключах**.

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.

Ключевые документы уничтожаются либо пользователями СКЗИ, либо сотрудниками органа криптографической защиты под расписку в соответствующих журналах поэкземплярного учета, а уничтожение большого объема ключевых документов может быть оформлено актом. При этом пользователям СКЗИ разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. После уничтожения пользователи СКЗИ должны уведомить об этом (телефонограммой, устным сообщением по телефону и т.п.) соответствующий орган криптографической защиты для списания уничтоженных документов с их лицевых счетов. Не реже одного раза в год пользователи СКЗИ должны направлять в орган криптографической защиты письменные отчеты об уничтоженных ключевых документах. Орган криптографической защиты вправе устанавливать периодичность представления указанных отчетов чаще одного раза в год.

Уничтожение по акту производит комиссия в составе не менее двух человек из числа сотрудников органа криптографической защиты. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых ключевых документов, инсталлирующих СКЗИ носителей, эксплуатационной и технической документации. Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делаются отметки в соответствующих журналах поэкземплярного учета.

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 лицензиата ФАПСИ, использование скомпрометированных **криптоключей**. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а передаваемая информация как можно менее ценной.

О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной 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.

Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, передававшейся (хранящейся) с использованием СКЗИ,

организует и осуществляет обладатель скомпрометированной конфиденциальной информации.

4. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним

Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним, должны обеспечивать сохранность конфиденциальной информации, СКЗИ, ключевых документов.

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

Требования к помещениям могут не предъявляться, если это предусмотрено правилами пользования СКЗИ, согласованными с ФАПСИ.

На время отсутствия пользователей СКЗИ оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае пользователи СКЗИ по согласованию с органом криптографической защиты обязаны предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами в их отсутствие.

Режим охраны помещений пользователей СКЗИ, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, устанавливает обладатель конфиденциальной информации.

Установленный режим охраны должен предусматривать периодический контроль за состоянием технических средств охраны, если таковые имеются, а также учитывать специфику и условия работы конкретных пользователей СКЗИ.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено руководству обладателя конфиденциальной информации 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 конфиденциальной информации и к замене скомпрометированных **криптоключей**.

***