Приложение № 2

УТВЕРЖДЕНА

распоряжением администрации

Анучинского муниципального округа

Приморского края

от «16» декабря 2020г. № 135-р

**Инструкция по обеспечению безопасности эксплуатации СКЗИ   
в администрации Анучинского муниципального округа  
 Приморского края**

1. ОБЩИЕ ПОЛОЖЕНИЯ
   1. Настоящая Инструкция определяет порядок учета, хранения и использования средств криптографической защиты информации (далее - СКЗИ), криптографических ключей и ключевых документов, а также порядок изготовления, смены, уничтожения и компрометации криптографических ключей в целях обеспечения безопасности эксплуатации СКЗИ.
   2. Настоящая Инструкция разработана в соответствии со следующими нормативными правовыми актами Российской Федерации:

* «Состав и содержание 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», утвержденного приказом ФСБ России от 10.07.2014 № 378;
* «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденное приказом ФСБ России от 09.02.2005 № 66);
* «Инструкция 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», утвержденная приказом ФАПСИ от 13.06.2001 № 152.
  1. В администрации Анучинского муниципального округа Приморского края (далее-Администрация АМО) используются только сертифицированные ФСБ России СКЗИ, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну.
  2. В Администрации АМО распоряжением администрации Анучинского муниципального округа Приморского края назначается ответственный за хранение и эксплуатацию СКЗИ, именуемый также органом криптографической защиты информации (далее – ОКЗ).
  3. Подписывая лист ознакомления с настоящей Инструкцией, ОКЗ подтверждает, что также ознакомлен 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 (утв. приказом ФАПСИ от 13.06.2001   
     № 152).
  4. ОКЗ осуществляет:
* поэкземплярный учет СКЗИ, эксплуатационной и технической документации к ним, ключевых носителей и ключевых документов;
* учет пользователей СКЗИ (далее – Пользователи) и представление на утверждение Главе Анучинского муниципального округа списка пользователей СКЗИ;
* контроль за соблюдением условий использования СКЗИ;
* расследования и составление заключений по фактам нарушений условий использования СКЗИ;
* разработку и обеспечение мер по предотвращению возможных нежелательных последствий таких нарушений;
* обучение Пользователей правилам работы с СКЗИ и правилам хранения СКЗИ, ключевых носителей и ключевых документов.
* хранение ключевой информации в сейфе;
  1. Список Пользователей утверждается Главой Анучинского муниципального округа.
  2. Пользователь обязан:
* не разглашать конфиденциальную информацию, к которой он допущен, в том числе: сведения об СКЗИ, ключевых документах к ним и других мерах защиты;
* соблюдать требования по обеспечению безопасности конфиденциальной информации при использовании СКЗИ;
* сообщать ОКЗ о попытках посторонних лиц получить сведения об СКЗИ или ключевых документах к ним установленных в реестре Windows;
* запрещается оставлять без контроля вычислительные средства  
  с установленным СКЗИ.
  1. К работе с СКЗИ Пользователи допускаются только после соответствующего инструктажа.

1. УЧЕТ СКЗИ, ХРАНЕНИЕ И ПЕРЕДАЧА КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ
   1. СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы и ключевые носители подлежат поэкземплярному учету. Программные СКЗИ учитываются совместно с аппаратными средствами, на которых осуществляется их штатная эксплуатация. Учет осуществляется ОКЗ в Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов (далее – Журнал).
   2. Единицей поэкземплярного учета ключевых документов считается отчуждаемый носитель с записанными криптографическими ключами. Если один и тот же носитель используется для записи другого криптографического ключа, его необходимо зарегистрировать снова.
   3. Дистрибутивы СКЗИ, эксплуатационная и техническая документация к ним, ключевые носители с криптографическими ключами хранятся у ОКЗ.
   4. Хранение осуществляется в сейфе индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.
   5. Ключевые носители с неработоспособными криптографическими ключами подлежат уничтожению. ОКЗ делает соответствующую запись в Журнале.
   6. **Аппаратные средства, с которыми осуществляется штатное использование СКЗИ, а также аппаратные СКЗИ должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) СКЗИ и аппаратных средств должно быть визуально контролируемым**.
2. ИСПОЛЬЗОВАНИЕ СКЗИ
   1. В Администрации АМО СКЗИ используется с целью обеспечения конфиденциальности и целостности электронных документов и сетевого трафика.
   2. Для шифрования электронного документа и/или сетевого трафика Пользователь использует свой собственный закрытый криптографический ключ и открытый криптографический ключ.
   3. В Администрации АМО используются только те СКЗИ, которые реализуют стойкие криптографические алгоритмы, не позволяющие в разумные сроки вычислить закрытый ключ по открытому ключу.
   4. Пользователь ежедневно проверяет сохранность технических средств и целостность печатей и пломб на них.
   5. В случае обнаружения неразрешенного программного обеспечения или факта повреждения целостности печати (пломбы) на техническом средстве с СКЗИ, работа с СКЗИ на таком техническом средстве должна быть прекращена. По данному факту созывается группа реагирования на инциденты информационной безопасности (далее – ГРИИБ), которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.
   6. Вскрытие технического средства с СКЗИ для проведения ремонта или технического обслуживания осуществляется только в присутствии ОКЗ.
   7. При работе с СКЗИ запрещается:

* оставлять без присмотра (контроля) технические средства, на которых эксплуатируется СКЗИ;
* самостоятельно вносить изменения в программную часть СКЗИ;
* разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и другие средства вывода информации;
* использовать ключевые носители в режимах, не предусмотренных штатными функциями СКЗИ;
* осуществлять несанкционированное копирование криптографических ключей;
* изменять настройки или пытаться изменить настройки СКЗИ или операционной системы, сделанные ОКЗ;
* использовать бывшие в работе ключевые носители для записи новой информации без предварительного гарантированного уничтожения на них ключевой информации;
* осуществлять самостоятельное несанкционированное вскрытие технических средств с СКЗИ.
  1. С целью обеспечения непрерывности работы Администрации АМО плановая замена ключевой информации должна производиться заблаговременно.

1. ДЕЙСТВИЯ ПРИ КОМПРОМЕТАЦИИ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ
   1. Криптографические ключи считаются скомпрометированными в следующих случаях:

* потеря ключевых носителей (в том числе с последующим обнаружением);
* увольнение сотрудников, имевших доступ к ключевым носителям;
* возникновение подозрений на утечку информации или ее искажение в информационной системе;
* нарушение печати на хранилище с ключевыми носителями ли на техническом средстве с СКЗИ;
* временный бесконтрольный доступ посторонних лиц к ключевым носителям или техническим средствам с СКЗИ;
* иные случаи подозрения компрометации криптографических ключей.
  1. В случае подозрения в компрометации криптографических ключей, Пользователь должен немедленно прекратить эксплуатацию СКЗИ и продолжить ее только после замены криптографических ключей.
  2. Скомпрометированные криптографические ключи подлежат уничтожению.

1. УНИЧТОЖЕНИЕ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ
   1. Неиспользованные или выведенные из действия криптографические ключи подлежат уничтожению.
   2. Уничтожение криптографических ключей на ключевых носителях производятся комиссией в составе председателя и членов комиссии, назначенной Распоряжением Администрации Анучинского муниципального округа Приморского края.
   3. Криптографические ключи, записанные на машинные ключевые носители, уничтожаются методом гарантированного стирания информации на машинном носителе в соответствии с требованиями эксплуатационной и технической документации на СКЗИ.
   4. Криптографические ключи, записанные на бумажных носителях, уничтожаются физически (сжигание, измельчение и т. д.).
   5. Перед уничтожением криптографических ключей и/или ключевых носителей, комиссия обязана:

* установить наличие оригинала и количество копий криптографических ключей;
* проверить внешнюю целостность каждого ключевого носителя;
* идентифицировать каждый ключевой носитель в соответствии с Журналом поэкземплярного учета средств криптографической защиты информации;
* убедиться, что криптографические ключи, находящиеся на ключевых носителях, действительно подлежат уничтожению;
* произвести уничтожение криптографических ключей на оригинале и всех копиях ключевого носителя.
  1. По факту уничтожения криптографических ключей составляется Акт уничтожения (Приложение № 3).
  2. Акт подписывается председателем и членами комиссии по уничтожению.
  3. В Журнале поэкземплярного учета средств криптографической защиты информации делается отметка об уничтожении криптографических ключей.
  4. Акты уничтожения криптографических ключей хранятся у ОКЗ.

1. ТРЕБОВАНИЯ К ПОМЕЩЕНИЯМ, В КОТОРЫХ ВЕДЕТСЯ РАБОТА С СКЗИ И/ИЛИ ХРАНЯТСЯ КРИПТОГРАФИЧЕСКИЕ КЛЮЧИ
   1. Помещения должны иметь прочные входные двери с замками, гарантирующими надежную защиту от проникновения посторонних лиц 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 посторонних лиц, необходимо оборудовать средствами, препятствующими неконтролируемому проникновению в помещения. При этом, применение нераспахиваемых железных решеток на окнах запрещено, поскольку это противоречит правилам пожарной безопасности.
   2. Мониторы рабочих станций с СКЗИ должны быть повернуты задней стороной к дверям и окнам, либо должны применяться шторы, рольставни, жалюзи или другие средства для пресечения несанкционированного просмотра содержимого, отображаемого на мониторах.
   3. Для хранения криптографических ключей, эксплуатационной и технической документации, дистрибутивов СКЗИ выделяется надежное металлическое хранилище (сейф). Ключи от хранилища хранятся у ОКЗ.
   4. По окончании рабочего дня помещение и хранилище должны быть закрыты на замок.
   5. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в помещение или хранилище посторонних лиц, ОКЗ немедленно должен оценить вероятность компрометации хранящихся криптографических ключей, составить акт и принять, при необходимости, меры к локализации последствия компрометации криптографических ключей и к их замене.

Приложение № 3

УТВЕРЖДЕН

Распоряжением администрации

Анучинского муниципального округа

Приморского края

от «16» декабря 2020г. № 135-р

**Акт установки средств криптографической защиты информации, вводав эксплуатацию и закрепления их за ответственными лицами**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование населенного пункта) (дата, месяц, год)

Настоящий акт составлен о том, что \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_сотрудником

(дата)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование организации, должность, Ф.И.О, иные сведения (например, дата, номер лицензии))(ответственный за эксплуатацию СКЗИ)

была произведена установка и настройка средств криптографической защиты информации \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
 (наименование)

далее -СКЗИ на ПЭВМ (АРМ Заявителя):

Серийный № (Инв. №) ПЭВМ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Место установки \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
 (адрес местонахождения, номер помещения)

Ф.И.О. пользователя АРМ Заявителя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
 (должность, фамилия, имя, отчество)(далее -пользователь СКЗИ)

Рег. № СКЗИ (номер экземпляра) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Обучение правилам работы с СКЗИ и проверка знаний нормативно-правовых актов и эксплуатационной и технической документации к ним проведены. Условия для использования СКЗИ, установленные эксплуатационной и технической документацией к СКЗИ, созданы. Установленное и настроенное СКЗИ находится в работоспособном состоянии.

Формуляр \_ \_ \_ \_. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ выведен на бумажный носитель, раздел 11 Формуляра заполнен установленным порядком, Формуляр хранится у ответственного за эксплуатацию СКЗИ.

Пользователь АРМ Заявителя обязуется:

−не разглашать конфиденциальную информацию, к которой он допущен, в том числе криптоключи и сведения о ключевой информации;

−соблюдать требования к обеспечению безопасности СКЗИ и ключевых документов к ним;

−сообщать ответственному о попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
(должность ответственного за эксплуатацию СКЗИ) (подпись) (Ф.И.О.)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
(должность пользователя СКЗИ) (подпись) (Ф.И.О.)

Приложение № 4

УТВЕРЖДЕН

Распоряжением администрации

Анучинского муниципального округа

Приморского края

от «16» декабря 2020г. № 135-р

**АКТ №\_\_\_\_\_ от «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_ г.**

**об уничтожении криптографических ключей и ключевых документов**

Комиссия в составе:

|  |
| --- |
| – председатель комиссии: |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| – члены комиссии: |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

произвела уничтожение криптографических ключей и ключевых документов:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№**  **п/п** | **Учетный номер ключевого носителя** | **Номер криптографи-ческого ключа, наименование документа** | **Владелец ключа (документа)** | **Количество ключевых носителей (документов)** | **Номера экземпляров** | **Всего ключей** | **Примечания** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

Всего уничтожено \_\_\_ криптографических ключей на \_\_\_ ключевых носителях. Записи Акта сверены с записями Журнала поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов.

Уничтожение криптографических ключей выполнено путем стирания (разрушения) по технологии, принятой для ключевых носителей многократного использования в соответствии с требованиями эксплуатационной и технической документации на соответствующие СКЗИ.

Ключевые носители списаны с учета в Журнале поэкземплярного учета средств криптографической защиты информации.

Председатель Комиссии :

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Члены Комиссии:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_