МУНИЦИПАЛЬНОЕ ОБРАЗОВАНИЕ  
 «УСТЬ-ЧИЖАПСКОЕ СЕЛЬСКОЕ ПОСЕЛЕНИЕ»

КАРГАСОСКИЙ РАЙОН ТОМСКАЯ ОБЛАСТЬ

**АДМИНИСТРАЦИИ УСТЬ-ЧИЖАПСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ**

**РАСПОРЯЖЕНИЕ**

|  |  |  |
| --- | --- | --- |
| 01.08.2019  с. Старая Берёзовка  Об утверждении Правил работы с средствами криптографической защиты информации в Администрации Усть-Чижапского сельского поселения |  | № 36 |

В целях исполнения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»

1.Назначить ответственными за организацию работ по криптографической защите информации инженеров-программистов хозяйственного отдела Администрации Каргасокского района.(по согласованию)

2. Утвердить Инструкцию ответственного за организацию работ по криптографической защите информации в Администрации Усть-Чижапского сельского поселения согласно приложению № 1 к настоящему распоряжению.

3. Утвердить Инструкцию по обращению со средствами криптографической защиты информации согласно приложению № 2 к настоящему распоряжению.

4. Утвердить Перечень пользователей средств криптографической защиты информации согласно приложению № 3 к настоящему распоряжению.

5. Утвердить форму Акта об уничтожении криптографических ключей, содержащихся на ключевых носителях, и ключевых документов согласно приложению № 4 к настоящему распоряжению.

6. Специалисту 1 категории Администрации Усть-Чижапского сельского поселения Алексеевой Д.И. ознакомить с настоящим распоряжением всех работников Администрации Усть-Чижапского сельского поселения, осуществляющих обработку персональных данных, под роспись.

|  |  |
| --- | --- |
| Глава Администрации Усть-Чижапского сельского поселения | С.М. Голещихин |

УТВЕРЖДЕНА

распоряжением Администрации Усть-Чижапского сельского поселения

от 01.08.2019 № 36

Приложение № 1

Инструкция ответственного за организацию работ

по криптографической защите информации в Администрации Усть-Чижапского сельского поселения

* **Общее положение**

Настоящая Инструкция разработана в целях регламентации действий лиц, ответственных за организацию работ по криптографической защите информации (далее – Ответственный) в Администрации Усть-Чижапского сельского поселения (далее – Администрация), которые осуществляют работы с применением средств криптографической защиты информации (далее – СКЗИ).

Под работами с применением СКЗИ в настоящей Инструкции понимаются защищенное подключение к информационным системам, подписание электронных документов электронной подписью и проверка подписи, шифрование файлов и т.д.

СКЗИ должны использоваться для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

* **Термины и определения**

Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами;

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

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 документ – физический носитель определенной структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости – контрольную, служебную и технологическую информацию;

Компрометация – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с криптоключами и ключевыми носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам;

Персональный компьютер (далее – ПК) – вычислительная машина, предназначенная для эксплуатации пользователем Администрации в рамках исполнения должностных обязанностей;

Пользователи СКЗИ – работники/сотрудники Администрации, непосредственно допущенные к работе с СКЗИ;

Средство криптографической защиты информации – совокупность аппаратных и (или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении;

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

* **Обязанности Ответственного**

При решении всех вопросов, связанных с обеспечением в Администрации безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа, Ответственный должен руководствоваться Инструкцией по обращению с СКЗИ.

**На Ответственного возлагается проведение следующих мероприятий:**

Ведение Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

**Ответственный обязан:**

1. Не разглашать информацию ограниченного доступа, к которой он допущен, в том числе сведения о криптоключах;
2. Незамедлительно принимать меры по локализации последствий компрометации защищаемых сведений конфиденциального характера;
3. Не допускать ввод одного номера лицензии на право использования СКЗИ более чем на одно рабочее место.

* **Права Ответственного**

В рамках исполнения возложенных на него обязанностей, Ответственный имеет право:

* Требовать от пользователей СКЗИ соблюдения положений Инструкции по обращению с СКЗИ;
* Инициировать проведение служебных расследований по фактам нарушения в Организации порядка обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

УТВЕРЖДЕНА

распоряжением Администрации

Усть-Чижапского сельского поселения от 01.08.2019 № 36

Приложение № 2

Инструкция по обращению со средствами криптографической

защиты информации

**1. Общее положение**

Настоящая Инструкция:

- разработана в целях регламентации действий лиц, допущенных к работе со средствами криптографической защиты информации (далее – СКЗИ) в Администрации Усть-Чижапского сельского поселения (далее – Администрация), которые осуществляют работы с применением СКЗИ;

- содержит рекомендации по размещению и хранению технических средств, на которые установлены СКЗИ;

- содержит рекомендации по проверке целостности установленного программного обеспечения (далее – ПО) СКЗИ, по использованию СКЗИ в различных автоматизированных системах.

Под работами с применением СКЗИ в настоящей Инструкции понимаются защищенное подключение к информационным системам, подписание электронных документов электронной подписью и проверка подписи, шифрование файлов и т.д.

Под обращением с СКЗИ в настоящей Инструкции понимается проведение мероприятий по обеспечению безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

СКЗИ должны использоваться для защиты информации ограниченного доступа (включая персональные данные), не содержащей сведений, составляющих государственную тайну.

Настоящая Инструкция в своем составе, терминах и определениях основывается на положениях «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», утвержденной приказом ФАПСИ от 13 июня 2001 г. №152 (далее – Инструкция ФАПСИ от 13 июня 2001 г. №152), «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ–2005)», утвержденного приказом ФСБ РФ от 9 февраля 2005 г. N 66.

**2. Сокращения, термины и определения**

Список сокращений

НСД - Несанкционированный доступ;

ОС - Операционная система;

ПО - Программное обеспечение;

ПЭВМ - Персональная электронная вычислительная машина;

СКЗИ - Средство криптографической защиты информации;

ТС - Технические средства;

ФСБ - Федеральная служба безопасности России;

ЭТД - Эксплуатационная и техническая документация.

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 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);

Компрометация – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с криптоключами и ключевыми носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам;

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

Персональный компьютер (далее – ПК) – вычислительная машина, предназначенная для эксплуатации пользователем Администрации в рамках исполнения должностных обязанностей;

Пользователи СКЗИ – работники Администрации, непосредственно допущенные к работе с СКЗИ;

Средство криптографической защиты информации – совокупность аппаратных и (или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при ее обработке и хранении;

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

**3. Работа с СКЗИ**

Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с СКЗИ, в помещениях пользователей СКЗИ 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 СКЗИ. На время отсутствия пользователей СКЗИ указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи. Для исключения утраты ключевой информации вследствие дефектов носителей рекомендуется, после получения ключевых носителей, создать рабочие копии. Копии должны быть соответствующим образом маркированы и должны использоваться, учитываться и храниться так же, как оригиналы.

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

При обнаружении на рабочем месте, оборудованном СКЗИ, посторонних программ или вирусов, нарушающих работу указанных средств, работа со СКЗИ на данном рабочем месте должна быть прекращена и организуются мероприятия по анализу и ликвидации негативных последствий данного нарушения.

**4. Действия в случае компрометации ключей**

О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием информации ограниченного доступа, пользователи СКЗИ обязаны информировать Постоянно действующую комиссии по обеспечению безопасности персональных данных, обрабатываемых в Администрации Усть-Чижапского сельского поселения.

К компрометации ключей относятся следующие события:

1. утрата носителей ключа;
2. утрата иных носителей ключа с последующим обнаружением;
3. увольнение сотрудников, имевших доступ к ключевой информации;
4. возникновение подозрений на утечку информации или ее искажение;
5. нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура опечатывания сейфов;
6. утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;
7. утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;
8. доступ посторонних лиц к ключевой информации;
9. другие события утери доверия к ключевой документации.

Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия.

Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их чтения, копирования. В случаях недостачи, не предъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

Мероприятия по розыску и локализации последствий компрометации информации ограниченного доступа, передававшейся (хранящейся) с использованием СКЗИ, организует и осуществляет Администрация.

**5. Обязанности и ответственность лиц, допущенных к работе с СКЗИ**

Лица, допущенные к работе с СКЗИ, обязаны:

* Не разглашать информацию ограниченного доступа, к которой они допущены, в том числе сведения о криптоключах;
* Сохранять носители ключевой информации и другие документы о ключах, выдаваемых с ключевыми носителями;
* Соблюдать требования к обеспечению с использованием СКЗИ безопасности информации ограниченного доступа;
* Немедленно уведомлять ответственного 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;
* Не вводить номера лицензий на СКЗИ, уже вводимые на других АРМ.

Лица, допущенные к работе с СКЗИ, отвечают за исполнение своих функциональных обязанностей и сохранность информации ограниченного доступа, которая стала ему известной вследствие исполнения им своих служебных обязанностей.

Ответственность лиц, допущенных к работе с СКЗИ, за неисполнение и (или) ненадлежащее исполнение своих обязанностей, предусмотренных соответствующими инструкциями (Инструкция ответственного за организацию работ по криптографической защите информации, Инструкция пользователя СКЗИ), а также за разглашение информации ограниченного доступа, ставшей ему известной вследствие исполнения им своих служебных обязанностей, определяется действующим законодательством Российской Федерации и условиями трудового договора.

УТВЕРЖДЕН

распоряжением Администрации

Усть-Чижапского сельского поселения от 01.08..2019 № 36

Приложение № 3

Перечень пользователей СКЗИ

|  |  |
| --- | --- |
| **Ф.И.О. должностного лица** | **Наименование должности** |
| **Работники отдела бухгалтерского учета и отчетности**  **Администрации Усть-Чижапского сельского поселения** | |
| Ольшанская И.С. | Главный бухгалтер |
| **Специалисты Администрации Усть-Чижапского сельского поселения** | |
| Алексеева Д.И. | Специалист 1 категории |
| Черевко А.В. | Специалист 2 категории |

УТВЕРЖДЕН

распоряжением Администрации

Усть-Чижапского сельского поселения от 01.08.2019 № 36

Приложение № 4

Акт № \_\_\_\_\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_20\_\_\_\_\_ г.

об уничтожении криптографических ключей,

содержащихся на ключевых носителях, и ключевых документов

Постоянно действующая комиссия по обеспечению безопасности персональных данных, обрабатываемых в Администрации Усть-Чижапского сельского поселения в составе:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

произвела уничтожение криптографических ключей, содержащихся на ключевых носителях, и ключевых документов:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | Учетный  номер  ключевого  носителя | Номер  (идентификатор)  криптографического  ключа | Владелец ключа | Количество  ключевых  носителей | Номера  экземпляров | Всего  уничтожается ключей |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Всего уничтожено \_\_\_\_\_\_\_ криптографических ключей на \_\_\_\_\_\_\_ ключевых носителях.

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

Записи Акта сверены с записями в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов.

Факт списания с учета ключевых носителей в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов **подтверждаю**:

|  |  |
| --- | --- |
| Ответственный за организацию работ по криптографической защите информации | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |  |
| --- | --- |
|  | Члены комиссии: |
|  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |