|  |  |  |
| --- | --- | --- |
| **Администрация муниципального образования**  **сельского поселения**  **«Намск»** |  | **«Нам»**  **сикт овмöдчöминлöн**  **муниципальной юконса администрация** |
| **РАСПОРЯЖЕНИЕ**  **ТШÖКТОМ** | | |

**от 22 марта 2021 года № 12-р**

(Республика Коми, Корткеросский район, п. Намск)

**Об обращении со средствами криптографической**

**защиты информации**

В целях исполнения требований «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

1. Назначить ответственным за организацию работ по криптографической защите информации в Администрации сельского поселения «Намск»:

- главу сельского поселения – Забоеву Светлану Валентиновну;

- главного бухгалтера администрации сельского поселения «Намск» - Михееву Екатерину Петровну;

- ведущего эксперта администрации сельского поселения «Намск» - Борисову Надежду Владимировну.

2. Утвердить Инструкцию ответственного за организацию работ по криптографической защите информации (Приложение №1).

3. Ответственному за организацию работ по криптографической защите информации ознакомиться под роспись и руководствоваться в своей деятельности Инструкцией ответственного за организацию работ по криптографической защите информации.

4. Утвердить Инструкцию по обращению со средствами криптографической защиты информации (далее - СКЗИ) (Приложение №2).

5. Ответственному за организацию работ по криптографической защите информации ознакомлять под роспись пользователей СКЗИ с Инструкцией по обращению с СКЗИ.

7. Пользователям, которым необходимо получить доступ к работе с СКЗИ, пройти обучение правилам работы с СКЗИ.

8. Утвердить Перечень пользователей СКЗИ (отдельным распоряжением в двух экземплярах).

9. Утвердить форму Журнала поэкземплярного учета СКЗИ (Приложение №3).

10. Контроль за исполнением настоящего Распоряжения оставляю за собой.

Глава сельского поселения \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_С.В. Забоева

Приложение

К распоряжению администрации

сельского поселения «Намск»

от 22.03.2021г. № 12-р

**ИНСТРУКЦИЯ**

**ответственного за организацию работ по криптографической защите информации**

1. **Общие положения**

Настоящая Инструкция разработана в целях регламентации действий лица, ответственного за организацию работ по криптографической защите информации (далее – Ответственный) в Администрации сельского поселения «Намск» (далее- Администрация), которое осуществляет 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.

Ответственный назначается Распоряжением Главы сельского поселения «Намск» из числа её работников.

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, «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 руководством 8 Центра ФСБ России 21 февраля 2008 г. №149/6/6-622.

1. **Термины и определения**

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 (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 (СКЗИ) - 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.

1. **Порядок получения допуска пользователей к работе с СКЗИ**

Для работы пользователей с СКЗИ в Администрации необходимо реализовать ряд мероприятий:

- пользователям, которым необходимо получить доступ к работе с СКЗИ, пройти самостоятельное обучение правилам работы с СКЗИ и тестирование на знание этих правил;

- издать Приказ об утверждении перечня пользователей СКЗИ;

- утвердить Инструкцию по обращению с СКЗИ;

- ознакомить всех пользователей СКЗИ с Инструкцией по обращению с СКЗИ под роспись.

Контроль над реализацией данных мероприятий возлагается на Ответственного.

1. **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, которая утверждается Приказом об обращении с СКЗИ.

**На Ответственного возлагается проведение следующих мероприятий:**

- вести Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

- вести учет актов об установке и настройке СЗИ;

- вести учет лицензий на право использования СКЗИ и соответствующих им Актов приема-передачи;

- принять СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы от пользователя при его увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

- осуществлять ежегодную проверку журнала учета СКЗИ, перечня пользователей СКЗИ и иных документов;

**Ответственный обязан:**

- не разглашать информацию ограниченного доступа, к которой он допущен, 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;

- контролировать целостность печатей (пломб) на технических средствах с установленными СКЗИ;

- незамедлительно принимать меры по локализации последствий компрометации защищаемых сведений конфиденциального характера;

- не допускать ввод одного номера лицензии на право использования СКЗИ более чем на одно рабочее место.

- обеспечивать централизованное хранение в специально выделенном хранилище дубликатов ключей от запираемых хранилищ пользователей ключевых носителей СКЗИ, а также их учет по Журналу сдачи и приема экземпляров ключей от запираемых хранилищ. Дубликат ключа хранится в закрытом конверте, на котором указываются фамилия, имя, отчество пользователя СКЗИ, номер помещения, в котором находится хранилище, и инвентарный номер хранилища.

1. **Права Ответственного**

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

- требовать от пользователей СКЗИ соблюдения положений Инструкции по обращению с СКЗИ;

- обращаться к главе сельского поселения «Намск» с требованием прекращения работы пользователя с СКЗИ при невыполнении им установленных требований по обращению с СКЗИ;

- инициировать проведение служебных расследований по фактам нарушения Администрации порядка обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа.

1. **Порядок передачи обязанностей при смене Ответственного**

При смене Ответственного должны быть внесены соответствующие изменения в Приказ об обращении с СКЗИ. Вновь назначенный Ответственный должен быть ознакомлен под роспись с настоящей Инструкцией и приступить к исполнению возложенных на него обязанностей.

1. **Заключительные положения**

Ознакомление с нормативными документами в области СКЗИ возможно на сайте ГАУ РК «ЦИТ» (http://www.test.cit.rkomi.ru).

**ЛИСТ ОЗНАКОМЛЕНИЯ**  
с Инструкцией ответственного за организацию работ

по криптографической защите информации

(утверждена Распоряжением АСП «Намск» от 22.03.2021 № 12)

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **ФИО** | **Должность** | **Дата/Подпись** |
| 1. |  |  |  |
| 2. |  |  |  |
| 3. |  |  |  |
| 4. |  |  |  |
| 5. |  |  |  |

Приложение 2

к распоряжению администрации

сельского поселения «Намск»

от 22 марта 2021 года № 12-р

**ИНСТРУКЦИЯ**

**по обращению со средствами криптографической защиты информации**

* 1. **Общие положения**

Настоящая Инструкция разработана в целях регламентации действий лиц, допущенных к работе со средствами криптографической защиты информации (далее - СКЗИ) в Администрации, которое осуществляет работы с применением 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.

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, «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 руководством 8 Центра ФСБ России 21 февраля 2008 г. №149/6/6-622.

* 1. **Термины и определения**

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 (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 (СКЗИ) - 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.

1. **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 и убрано в опечатываемые хранилища. В противном случае, в организации должны быть обеспечены условия хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации.

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 средствами защиты информации на данном рабочем месте должна быть прекращена и организуются мероприятия по анализу и ликвидации негативных последствий данного нарушения.

1. **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 сообщать Ответственному за организацию работ по криптографической защите информации.

К компрометации ключей относятся следующие события:

- утрата носителей ключа;

- утрата иных носителей ключа с последующим обнаружением;

- увольнение сотрудников, имевших доступ к ключевой информации;

- возникновение подозрений на утечку информации или ее искажение;

- нарушение целостности печатей на сейфах с носителями ключевой информации, если используется процедура опечатывания сейфов;

- утрата ключей от сейфов в момент нахождения в них носителей ключевой информации;

- утрата ключей от сейфов в момент нахождения в них носителей ключевой информации с последующим обнаружением;

- доступ посторонних лиц к ключевой информации;

- 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 копирования (чтения, размножения). 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 (обладатель скомпрометированной информации ограниченного доступа).

1. **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 информс

руководству о ставших ему известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

- в случае необходимости производить уничтожение криптоключей и ключевых документов в соответствии с требованиями пунктов 41-46 Инструкции ФАПСИ от 13 июня 2001 г. №152.

- не вводить номера лицензий на СКЗИ, уже вводимые на других АРМ;

- по окончании рабочего дня убирать ключевые носители в запираемые шкафы, ящики столов или сейфы (далее – хранилища). Пользователь не имеет права без письменного указания Ответственного за организацию работ по криптографической защите передавать ключ от хранилища третьим лицам и несет ответственность за его сохранность. Дубликат ключа от хранилища необходимо передать Ответственному за организацию работ по криптографической защите с записью в Журнале сдачи и приема экземпляров ключей от запираемых хранилищ.

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.

1. **Заключительные положения**

Контактная информация

**ЛИСТ ОЗНАКОМЛЕНИЯ**

с Инструкцией по обращению со средствами

криптографической защиты информации

(утверждена Распоряжением АСП «Намск» от 22.03.2021 № 12)

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **ФИО** | **Должность** | **Дата/Подпись** |
| 1. |  |  |  |
| 2. |  |  |  |
| 3. |  |  |  |
| 4. |  |  |  |
| 5. |  |  |  |

|  |  |
| --- | --- |
|  | Приложение № 3  к Распоряжению  Администрации сельского поселения «Намск»  от 22.03.2021г. № 12  (форма) |

**Администрация сельского поселения «Намск»**

|  |  |
| --- | --- |
|  | УТВЕРЖДАЮ  Глава сельского поселения «Намск»  \_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_г. |

**ЖУРНАЛ №\_\_\_**

**поэкземплярного учета средств криптографической защиты информации**

Журнал начат «\_\_»\_\_\_\_\_\_\_\_\_\_\_ 201\_\_\_года

Журнал завершен «\_\_»\_\_\_\_\_\_\_\_\_\_\_20\_\_ года

На \_\_\_ листах

п. Намск, 20\_\_\_\_\_\_г.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Наименование СКЗИ | Лицензионный/серийный номер СКЗИ | Учетный номер  дистрибутива СКЗИ | Отметка о получении | | Отметка о подключении (установке СКЗИ) | | | | Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов | | Примечание |
| Наименование организации, передавшей СКЗИ | Номер и дата документа, подтверждающего получение СКЗИ | Ф.И.О. пользователя СКЗИ | Ф.И.О. сотрудника, установившего СКЗИ | Дата подключения (установки) СКЗИ, расписка об установке | Инв. номер аппаратных средств, на которые установлены СКЗИ | Ф.И.О. сотрудника, производившего изъятие (уничтожение) СКЗИ | Дата изъятия (удаления) СКЗИ, расписка об уничтожении (удалении) |  |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |