Приложение 7

к постановлению администрации
сельского поселения «Слудка»
от 29.08.2014г № 8/43

# ИНСТРУКЦИЯ
пользователя по обращению со средствами криптографической защиты информации (СКЗИ)

## 1.Общие положения

1.1 Настоящая Инструкция определяет:
а) порядок обращения со средствами криптографической защиты информации (далее – СКЗИ) и криптографическими ключами;
б) основные обязанности, права и ответственность пользователя СКЗИ (далее – Пользователя);
в) действия при компрометации ключей и восстановлении конфиденциальной связи;
г) специальные требования по обработке информации с использованием СКЗИ;
1.2 Пользователь должен выполнять все требования настоящей Инструкции, правила, изложенные в эксплуатационной документации на СКЗИ, а также другие документы, регламентирующие порядок работы с СКЗИ.
1.3 Деятельность Пользователя по вопросам обращения со СКЗИ контролируется непосредственным руководителем структурного подразделения и работником отдела общего обеспечения (далее – Администратор СКЗИ).
1.4 Администратор СКЗИ назначается и смещается приказом руководителя Администрации. Обязанности, права и ответственность Администратора СКЗИ устанавливаются отдельным нормативным актом Администрации.
1.5 СКЗИ и средства ЭЦП могут использоваться для защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну.

## 2. Основные обязанности Пользователя

2.1. Пользователь обязан:
а) соблюдать требования по обеспечению безопасности функционирования СКЗИ;
б) обеспечить конфиденциальность всей информации ограниченного распространения, доступной по роду выполняемых функциональных обязанностей;
в) сдать руководителю структурного подразделения или Администратору СКЗИ носители ключевой информации (далее – НКИ) при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;
г) сдать руководителю структурного подразделения или Администратору СКЗИ НКИ по окончании срока действия сертификата ключа, а также в случае компрометации ключа;
д) немедленно уведомлять руководителя структурного подразделения и Администратора СКЗИ о случаях компрометации криптографических ключей;
е) немедленно уведомлять руководителя структурного подразделения и Администратора СКЗИ о фактах утраты или недостачи СКЗИ, НКИ;

ж) в пределах своей компетенции предоставлять информацию комиссии, проводящей служебные расследования по фактам компрометации, а также выявлению причин нарушения требований безопасности функционирования СКЗИ.

## 3. Права Пользователя

3.1. Пользователь имеет право:
а) вносить предложения по совершенствованию СКЗИ;
б) повышать уровень квалификации по использованию СКЗИ.

## 4. Порядок обращения со СКЗИ

4.1 Монтаж и установка СКЗИ осуществляются уполномоченным лицом – Администратором СКЗИ или представителем оператора безопасности Республики Коми - ГБУ Республики Коми «Центр безопасности информации».
4.2 Служебные помещения (кабинеты), в которых размещаются СКЗИ, должны отвечать всем требованиям по оборудованию и охране, предъявляемым к помещениям, выделенным для работы с конфиденциальной информацией. Для хранения носителей ключевой информации помещения обеспечиваются запираемыми шкафами, сейфами (металлическими шкафами), по убытию работников закрываются и опломбируются.
4.3 К эксплуатации СКЗИ допускаются работники, прошедшие соответствующую подготовку и изучившие правила пользования СКЗИ и НКИ, изложенные в настоящей Инструкции.
4.4 Все программное обеспечение АРМ, предназначенное для установки СКЗИ, должно иметь соответствующие лицензии. Установка средств разработки и отладки программ на АРМ, использующее СКЗИ, не допускается.

## 5. Использование ЭЦП

5.1 Электронная цифровая подпись (далее - ЭЦП) – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.
5.2 Сертификат ключа подписи – документ на бумажном носителе или электронный документ с ЭЦП Удостоверяющего центра, которые включают в себя открытый ключ ЭЦП и которые выдаются Удостоверяющим центром участнику информационной системы для подтверждения подлинности ЭЦП и идентификации Владельца сертификата ключа подписи. Сертификат ключа подписи хранится у Владельца с соблюдением требований безопасности.
5.3 Владелец сертификата ключа подписи – физическое лицо, на имя которого Удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом ЭЦП, позволяющим с помощью средств ЭЦП создавать свою ЭЦП в электронных документах (подписывать электронные документы).
5.4 Подтверждение подлинности ЭЦП в электронном документе – положительный результат проверки соответствующим сертифицированным средством ЭЦП с использованием сертификата ключа подписи принадлежности ЭЦП в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

5.5 ЭЦП в электронном документе равнозначна собственноручной подписи владельца ключа в документе на бумажном носителе при одновременном соблюдении следующих условий:
а) сертификат ключа подписи, относящийся к этой ЭЦП, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
б) подтверждена подлинность электронной цифровой подписи в электронном документе;
в) электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

## 6. Порядок обращения с ключами ЭЦП

6.1 Криптографический ключ Владельца ключа применяется для подписания (проверки ЭЦП) электронных документов до окончания срока его действия или наступления события, трактуемого как компрометация криптоключей.
6.2 Владелец ЭЦП – Пользователь СКЗИ, получивший установленным порядком право использовать персональный ключ ЭЦП для удостоверения содержания электронных документов и своего авторства.
6.3 Доверенное лицо Владельца ЭЦП – пользователь СКЗИ, получивший установленным порядком право использовать ключ Владельца ЭЦП для удостоверения содержания электронных документов и авторства Владельца.
6.4 Назначение владельцев ЭЦП и доверенных лиц осуществляется на основании приказа руководителя Администрации о назначении пользователей СКЗИ.
6.5 Подготовку документации (подача заявки) для изготовления ключей ЭЦП осуществляется работником отдела общего обеспечения – Администратором СКЗИ. Получение ключа ЭЦП в Удостоверяющем центре выполняет лично Владелец ЭЦП или доверенное лицо Владельца ЭЦП.
6.6 Выработанные секретные криптоключи хранятся исключительно в электронном виде на цифровых носителях информации, которые получают статус НКИ.
6.7 НКИ являются объектами особой важности, т.к. они содержат информацию, предназначенную для гарантированной идентификации Владельца ключа, защиты электронного документа от подделки, компрометации.
6.8 Владельцы ключей (доверенные лица Владельца) несут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту НКИ от несанкционированного использования.
6.9 Для хранения носителей ключевой информации Пользователь должен быть обеспечен запираемым шкафом, сейфом (металлическими шкафами).
6.10 Пользователю категорически запрещается:
а) осуществлять несанкционированное и безучётное копирование ключевых данных;
б) хранить НКИ вне сейфов и помещений, гарантирующих их сохранность и конфиденциальность;
в) передавать НКИ каким бы то ни было лицам, кроме Владельца ключа;
г) во время работы оставлять НКИ без присмотра (например, на рабочем столе или в разъеме системного блока АРМ);
д) хранить на НКИ какую-либо информацию, кроме ключевой;
е) использование криптоключей, выведенных из действия;
ж) разглашать содержимое НКИ;
з) вносить какие-либо изменения в программное обеспечение СКЗИ и средств ЭЦП;
и) вставлять НКИ в интерфейс АРМ при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка ЭЦП и т.д.), а также в интерфейсы других АРМ.

6.11 Запрещается использовать НКИ на АРМ с не установленными программными средствами антивирусной защиты.

## 7. Действия при компрометации действующих ключей и восстановлении конфиденциальной связи

7.1 Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию Владельца и конфиденциальность информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих криптографических ключей, относятся:
а) утрата (хищение) НКИ, в том числе – с последующим их обнаружением;
б) увольнение (переназначение) сотрудников, имевших доступ к ключевой информации;
в) передача секретных ключей по линии связи в открытом виде;
г) нарушение правил хранения криптоключей;
д) вскрытие фактов утечки передаваемой информации или её искажения (подмены, подделки);
е) отрицательный результат при проверке наложенной ЭЦП;
ж) несанкционированное или безучётное копирование ключевой информации;
з) все случаи, когда нельзя достоверно установить, что произошло с НКИ (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий).

7.2 События 7.1.(а-д) должны трактоваться как безусловная компрометация действующих ключей. Остальные события требуют специального расследования в каждом конкретном случае.
7.3 При наступлении любого из перечисленных в п. 7.1 событий Владелец ключа должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации руководителю структурного подразделения или Администратору СКЗИ.
7.4 При подтверждении факта компрометации действующих ключей Пользователь обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей.
7.5 Для восстановления конфиденциальной связи, после компрометации действующих ключей, на Пользователя оформляются новые ключи ЭЦП.

## 8. Ответственность Пользователя

8.1. Владелец ключа несет персональную ответственность за обеспечение конфиденциальности личных ключевых носителей.
8.2 В случае неисполнения или ненадлежащего выполнения требований настоящей Инструкции Пользователь ключа может быть привлечен к дисциплинарной и/или административной ответственности в соответствии с действующим законодательством Российской Федерации.

Приложение

| п/п | Нештатная ситуация | Действие работника |
|---|---|---|
| 1. | Эвакуация, угроза взрыва или нападения, стихийные бедствия и т.д. | **- Остановить ПЭВМ.**<br>**- Сдать все имеющиеся ключевые носители** администрации или администратору СКЗИ.<br>- Администратор СКЗИ упаковывает все ключевые носители, регистрационные карточки открытых ключей в опечатываемый контейнер, который выносит в безопасное помещение/здание.<br>- Администратор СКЗИ оповещает всех пользователей о приостановки работы.<br>- В случае наступления события, повлекшего за собой долговременный выход из строя аппаратный средств, администратор СКЗИ уничтожает все ключевые носители, находящиеся в опечатываемом контейнере. |
| 2. | Компрометация одного из личных ключевых носителей. | **Смотри п.7 настоящей инструкции.** |
| 3. | Утеря личного носителя ключевой информации. | **Смотри п.7 настоящей инструкции.** |
| 4. | Выход из строя личного основного ключевого носителя (дискета). | **- Сообщить администратору СКЗИ о выходе из строя ключевого носителя.**<br>**- Обеспечить доставку основного ключевого носителя администратору СКЗИ для выяснения причин выхода его из строя.**<br>- Для работы использовать резервный ключевой носитель. |
| 5. | Выход из строя личного резервного ключевого носителя (дискета). | **- Сообщить администратору СКЗИ о выходе из строя резервного ключевого носителя.**<br>**- Обеспечить доставку резервного ключевого носителя администратору СКЗИ для выяснения причин выхода его из строя.**<br>**- Получение от администратора СКЗИ дубликата резервной копии ключевого носителя.** |
| 6. | Отказы и сбои в работе аппаратной части АРМ со встроенным СКЗИ. | **Необходимо остановить работу**, по возможности локализовать неисправность и выполнить ремонт. При необходимости переустановить СКЗИ. |
| 7. | Отказы и сбои в работе программных средств. | **Необходимо остановить работу**, по возможности локализовать неисправность. Устранить причину отказа ПО. При необходимости переустановить СКЗИ. |
| 8. | Отказы в работе программных средств вследствие случайного или умышленного их повреждения. | Администратор СКЗИ инициирует проведение служебного расследования по факту умышленного или случайного повреждения ПО с целью установления причин отказа. Выполнение работ по восстановлению работоспособности ПО. |