

ИНСТРУКЦИЯ

по обеспечению безопасности эксплуатации средств криптографической защиты информации (СКЗИ)

1. Общие положения

1.1. Настоящая Инструкция определяет порядок учета, хранения и использования средств криптографической защиты информации (СКЗИ) и криптографических ключей, а также порядок изготовления, смены, уничтожения и компрометации криптографических ключей в целях обеспечения безопасности эксплуатации в МБОУ г. Астрахани «СОШ№30».

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.

2. Обязанности Пользователя

2.1. Пользователь обязан соблюдать требования по обеспечению безопасности функционирования СКЗИ.

2.2. Пользователь обязан обеспечить конфиденциальность всей информации ограниченного распространения, доступной по роду выполняемых функциональных обязанностей.

2.3. Пользователь обязан сдать носители ключевой информации (далее – НКИ) при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ, ответственному за обработку персональных данных.

2.4. Пользователь обязан сдать носители ключевой информации (далее – НКИ) по окончании срока действия сертификата ключа, а также в случае компрометации ключа.

2.5. Пользователь обязан немедленно уведомлять Ответственного за обработку персональных данных о компрометации криптографических ключей.

2.6. Пользователь обязан немедленно уведомлять Ответственного за обработку персональных данных о фактах утраты или недостачи СКЗИ, НКИ.

3. Порядок обращения со средствами криптографической защиты информации

3.1. Монтаж и установка СКЗИ осуществляются только уполномоченным лицом, либо организацией, имеющей необходимые лицензии.

3.2. Все СКЗИ и НКИ должны учитываться в журнале.

3.3. Служебные помещения, в которых размещаются СКЗИ, должны оборудоваться охранной сигнализацией, по убытии сотрудников закрываться и сдаваться под охрану.

3.4. Для хранения носителей ключевой информации помещения обеспечиваются сейфами (металлическими шкафами).

3.5. Несанкционированное изготовление дубликатов ключей ЗАПРЕЩЕНО. В случае утери ключа механизм (секрет) замка (либо сам сейф) должен быть заменён.

3.6. К эксплуатации СКЗИ допускаются лица, изучившие правила пользования данным СКЗИ.

3.7. Все программное обеспечение ПЭВМ, предназначенной для установки СКЗИ, должно иметь соответствующие лицензии. Установка средств разработки и отладки программ на рабочую станцию, использующую СКЗИ, не допускается.

4. Порядок обращения с ключами ЭЦП

4.1. Криптографический ключ применяется для подписания (проверки электронной цифровой подписи) электронных документов до окончания срока его действия или наступления события, трактуемого как компрометация криптографических ключей.

4.2. Изготовление и выдача ключей ЭЦП осуществляется только Удостоверяющим центром.

4.3. Выработанные закрытые (конфиденциальные) криптографические ключи хранятся исключительно в электронном виде на цифровых носителях информации, которые получают статус НКИ.

4.4. НКИ являются объектами особой важности, т.к. они содержат информацию, предназначенную для гарантированной идентификации владельца ключа, защиты электронного документа от подделки и обеспечения конфиденциальности документа.

4.5. Владельцы ключей несут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту НКИ от несанкционированного использования.

4.6. Для хранения носителей ключевой информации Пользователь должен быть обеспечен личным сейфом.

5. Запрещается

5.1. Осуществлять несанкционированное и без учёта копирование ключевых данных.

5.2. Хранить НКИ вне сейфов и помещений, гарантирующих их сохранность и конфиденциальность.

5.3. Передавать НКИ третьим лицам.

5.4. Во время работы оставлять НКИ без присмотра (например, на рабочем столе или в разъеме системного блока ПЭВМ).

5.5. Хранить на НКИ какую-либо информацию, кроме ключевой.

5.6. Использование выведенных из действия криптографических ключей.

6. Действия при компрометации действующих ключей и восстановлении конфиденциальной связи

6.1. 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:

- Утрата (хищение) НКИ, в том числе – с последующим их обнаружением;
- Увольнение (переназначение) сотрудников, имевших доступ к ключевой информации;
- Передача закрытых (конфиденциальных) ключей по линии связи в открытом виде;
- Нарушение правил хранения криптографических ключей;
- Вскрытие фактов утечки передаваемой информации или её искажения (подмены, подделки);
- Отрицательный результат при проверке наложенной ЭЦП;
- Несанкционированное или без учёта копирование ключевой информации;
- 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 произошёл в результате злоумышленных действий).

6.2. При наступлении любого из перечисленных выше событий Владелец ключа должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) в Удостоверяющий центр, производивший генерацию ключей ЭЦП.

6.3. При подтверждении факта компрометации действующих ключей Пользователь обязан обеспечить немедленное изъятие из обращения

скомпрометированных криптографических ключей.

6.4. Для восстановления конфиденциальной связи после компрометации действующих ключей Пользователь получает в Удостоверяющем центре новые ключи ЭЦП.

7. Ответственность Пользователя

7.1. Владелец ключа несет персональную ответственность за конфиденциальность личных ключевых носителей.

7.2. В случае неисполнения или ненадлежащего выполнения требований настоящей Инструкции Пользователь несёт ответственность в соответствии с действующим Законодательством Российской Федерации.