

УТВЕРЖДАЮ
Управляющая делами
Администрации города Кургана
Н.А. Румянцева

« 21 » ноября 2012 г.

**ИНСТРУКЦИЯ ПО РАБОТЕ СО СРЕДСТВАМИ КРИПТОГРАФИЧЕСКОЙ
ЗАЩИТЫ ИНФОРМАЦИИ (СКЗИ) В АДМИНИСТРАЦИИ ГОРОДА КУРГАНА**

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция определяет основные принципы, меры и требования при работе со средствами криптографической защиты информации (далее – СКЗИ), эксплуатируемыми в информационных системах Администрации города Кургана.

1.2. Настоящая инструкция разработана на основе:

- Федерального закона Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ;

- Федерального закона Российской Федерации «Об электронной подписи» от 1 июля 2011 г. № 63-ФЗ

- Указа Президента Российской Федерации «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17 марта 2008 г. № 351;

- Приказа ФАПСИ «Об утверждении 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» от 13 июня 2001 г. № 152;

- «Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», утвержденного приказом ФСБ России от 9 февраля 2005 г. № 66. В качестве программно-аппаратного средства для создания УЦ Администрации города Кургана используется программно-аппаратный комплекс «Удостоверяющий центр «КриптоПро».

1.3. Системы электронного документооборота администрации города Кургана функционируют на основе сертифицированного ФСБ России СКЗИ «КриптоПро CSP» (вариант КС1).

1.4. СКЗИ «КриптоПро CSP» предназначено для авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями, посредством использования процедур формирования и проверки электронной подписи (далее – ЭП) в соответствии с отечественными стандартами ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001.

2. ИСПОЛЬЗОВАНИЕ СКЗИ И КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ

2.1. СКЗИ и криптографические ключи используются для обеспечения конфиденциальности, авторства и целостности электронных документов.

2.2. Конфиденциальность электронных документов обеспечивается путем их шифрования. Авторство и целостность электронных документов обеспечивается путем создания в документе ЭП Пользователя.

2.3. В системах электронного документооборота администрации города Кургана используется СКЗИ с открытым распределением ключей.

2.4. Электронный документ может быть подписан ЭП с использованием только того закрытого ключа ЭП, для которого Удостоверяющий центр (далее – УЦ) Администрации города Кургана выдал сертификат ключа подписи Пользователя.

2.5. Для операции подписи электронного документа Пользователь использует свой собственный закрытый криптографический ключ соответствующий открытому криптографическому ключу.

2.6. Открытый криптографический ключ содержится в сертификате ключа подписи, который выдает УЦ Администрации города Кургана Пользователю в электронной форме и на бумажном носителе (при необходимости).

2.7. Проверка подлинности ЭП электронного документа осуществляется Пользователем с использованием открытого криптографического ключа отправителя документа.

2.8. Пользователь не может подписать электронный документ своей ЭП если истек срок действия закрытых криптографических ключей. Также Пользователь не может проверить ЭП электронного документа или произвести его расшифрование в случае истечения срока действия сертификата ключа подписи, необходимого для выполнения соответствующей операции.

2.9. Реализованные в СКЗИ алгоритмы шифрования и электронной цифровой подписи гарантируют невозможность восстановления закрытых криптографических ключей отправителя по его открытым ключам.

2.10. Криптографические ключи изготавливаются на отчуждаемый ключевой носитель (eToken) в соответствии с эксплуатационно-технической документацией на СКЗИ и требованиями безопасности, установленными инструкцией по безопасной эксплуатации средств криптографической защиты информации.

2.11. Все полученные экземпляры СКЗИ, эксплуатационной и технической документации к ним, криптографических ключей выдаются под расписку в соответствующих журналах.

2.12. По окончании рабочего дня все полученные ключевые носители с СКЗИ должны помещаться в личный опечатываемый сейф Пользователя или сдаваться в опечатанном тубусе (при отсутствии у Пользователя СКЗИ сейфа) назначенному работнику Администрации города Кургана.

2.13. В случае возникновения обстоятельств, указывающих на возможную компрометацию криптографических ключей (утрату к ним доверия), Пользователь обязан немедленно прекратить обмен электронными документами с использованием скомпрометированных криптографических ключей и проинформировать Администратора безопасности и Ответственного пользователя криптосредств.

2.14. Неиспользованные, скомпрометированные или выведенные из действия криптографические ключи подлежат уничтожению.

