УТВЕРЖДАЮ
Управляющая делами
Администрации города Кургана
Н.А. Румянцева

«21» ноября 2012 г.

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЕЙ ПО БЕЗОПАСНОЙ ЭКСПЛУАТАЦИИ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИФОРМАЦИИ (СКЗИ) В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА АДМИНИСТРАЦИИ ГОРОДА КУРГАН

СОДЕРЖАНИЕ

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. В настоящей Инструкции по безопасной эксплуатации средств криптографической защиты информации в системах электронного документооборота (далее – Инструкция) применяются следующие термины и определения:

Средства криптографической защиты информации (СКЗИ, криптосредства) – совокупность программно-технических средств, обеспечивающих применение ЭП и/или шифрования при осуществлении электронного документооборота.

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

Безопасность эксплуатации СКЗИ – совокупность мер управления и контроля, защищающая СКЗИ и криптографические ключи от несанкционированного (умышленного или случайного) их раскрытия, модификации, разрушения или использования.

Электронный документ – документ, в котором информация имеющая смысл для Участников СЕД, представлена в электронно-цифровой форме в установленном Правилами ЭДО формате.

Электронный документооборот (ЭДО) – обмен электронными документами в соответствии с установленными правилами ЭДО.

Система электронного документооборота (СЭД) – организационно-техническая система, представляющая собой совокупность нормативного, программного, информационного и технического обеспечения.

Участник СЭД – юридическое или физическое лицо, участвующее в ЭДО.

Пользователь – Участник СЭД, который использует СКЗИ для обеспечения электронного документооборота в СЭД.

Ответственный пользователь криптосредств – работник или представитель Участника СЭД, осуществляющий организацию и обеспечение работ по техническому обслуживанию СКЗИ и управление криптографическими ключами Участника СЭД.

ПЭВМ – персональная электронно-вычислительная машина (персональный компьютер).

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящая инструкция определяет порядок использования СКЗИ и криптографических ключей, основные обязанности, права и ответственность Пользователей СКЗИ в целях обеспечения безопасности эксплуатации СКЗИ в СЭД.

2.2. 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.

2.3. В СЭД используются сертифицированные ФСБ России СКЗИ, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну, при обеспечении безопасности информации по уровню «КС1».

2.4. Для организации и обеспечения работ по техническому обслуживанию СКЗИ и управления криптографическими ключами приказом руководителя Участника СЭД назначается ответственный за безопасное функционирование СКЗИ - Ответственный пользователь криптосредств.

2.5. Пользователи СКЗИ назначаются приказом руководителя Участника СЭД и учитываются в соответствующем журнале.

2.6. Непосредственно к работе с СКЗИ Пользователи допускаются только после соответствующего обучения.

2.7. Обучение Пользователей правилам работы с СКЗИ осуществляет Ответственный пользователь криптосредств.

2.8. Пользователи Участника СЭД должны быть ознакомлены с настоящей Инструкцией под расписку.

3. ОБЯЗАННОСТИ ПОЛЬЗОВАТЛЯ

3.1. Пользователь СКЗИ обязан:

– обеспечивать конфиденциальность всей информации ограниченного распространения, доступной по роду выполняемых функциональных обязанностей, в том числе сведения о криптографических ключах;

– не допускать снятие копий с ключевых документов;

– не допускать записи посторонней информации на ключевой носитель;

– сдать Ответственному пользователю криптосредств носители ключевой информации при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

– сдать Ответственному пользователю криптосредств носители ключевой информации по окончании срока действия сертификата ключа, а также в случае компрометации ключа;

– незамедлительно уведомлять Ответственного пользователя криптосредств о фактах утраты или недостачи СКЗИ, криптографических ключей, 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;

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

3.2. Пользователю ЗАПРЕЩАЕТСЯ:

– осуществлять несанкционированное копирование криптографических ключей;

– использовать ключевые носители для работы на других рабочих местах или дляшифрования и подписи ЭД, не относящейся к работе в СЭД УЦ Администрации города Кургана;

– хранить ключевые носители вне сейфов и помещений, гарантирующих их сохранность и конфиденциальность;

– передавать ключевые носители каким бы то ни было лицам;

– во время работы оставлять ключевые носители без присмотра (например, на рабочем столе или в разъеме системного блока ПЭВМ);

– использовать в помещениях, где применяются СКЗИ, личные технические средства, позволяющие осуществлять копирование ключевой информации;

– разглашать содержимое носителей ключевой информации или выводить ключевую информацию на дисплей и принтер;

– вставлять носители криптографических ключей в устройства считывания в режимах, не предусмотренных штатным режимом работы СКЗИ;

– записывать на носители с криптографическими ключами постороннюю информацию;

– подключать к ПЭВМ дополнительные устройства и соединители, непредусмотренные в комплектации;

– вести работу на ПЭВМ, при обнаружении каких-либо неисправностей;

– вносить какие-либо изменения в программное обеспечение СКЗИ;

– вести работу на ПЭВМ при отключенных средствах антивирусной защиты.

4. ПРАВА ПОЛЬЗОВАТЕЛЯ

4.1. Пользователь имеет право:

– вносить предложения Руководству по совершенствованию СКЗИ;

– повышать уровень квалификации по использованию СКЗИ.

5. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЯ

5.1.Пользователь несет персональную ответственность за сохранность выданных ему ключевых носителей.

5.2.В случае неисполнения или ненадлежащего выполнения требований настоящей Инструкции Пользователь может быть привлечен к дисциплинарной и/или административной ответственности в соответствии с действующим Законодательством Российской Федерации.