ИНСТРУКЦИЯ

по использованию средств криптографической защиты информации и электронной подписи в системах передачи электронных документов по телекоммуникационным каналам связи

1. Общие положения

Средства криптографической защиты информации (СКЗИ) и электронной подписи (ЭП), входящие в состав комплекта программного обеспечения электронного документооборота, предназначены для подписания электронных документов ЭП с целью подтверждения подлинности информации, ее авторства и шифрования этих файлов при передаче по открытым каналам связи для обеспечения конфиденциальности.

Указанные СКЗИ и средства ЭП могут использоваться только для защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну.

2. Работа с СКЗИ и средствами ЭП в организациях, работающих в системах электронного документооборота

Для работы с СКЗИ и средствами ЭП привлекаются уполномоченные лица, назначенные соответствующим приказом руководителя организации. Должностные лица, уполномоченные соответствующим приказом руководителя организации эксплуатировать СКЗИ, получать и использовать ключи шифрования и ЭП, несут персональную ответственность за:

- сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы с СКЗИ;
- сохранение в тайне содержания закрытых ключей СКЗИ и средств ЭП;
- сохранность носителей ключевой информации и других документов о ключах, выдаваемых с ключевыми носителями.

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 их рабочие копии. Копии должны быть соответствующим образом маркированы и должны использоваться, учитываться и храниться так же, как оригиналы.

Пользователь несет ответственность за то, чтобы на ПЭВМ, на которой установлены СКЗИ и средства ЭП, не были установлены и не эксплуатировались программы (в том числе, программы-вирусы), которые могут нарушить функционирование программных СКЗИ и средств ЭП.

При обнаружении на рабочем месте, оборудованном СКЗИ и средствами ЭП, 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.

Не допускается:

- а) разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным;
- б) выводить ключевую информацию на дисплей и принтер;

- в) вставлять ключевой носитель в ПЭВМ при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной подписи и т.д.), а также в другие ПЭВМ;
- г) записывать на ключевом носителе постороннюю информацию;
- д) вносить какие-либо изменения в программное обеспечение СКЗИ и средств ЭП;
- е) использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования (рекомендуется физическое уничтожение носителей).

3. Действия в случае компрометации ключей

Под компрометацией закрытых ключей понимается их утрата (в том числе с их последующим обнаружением), хищение, разглашение, несанкционированное копирование, передача их по линии связи в открытом виде, увольнение по любой причине сотрудника, имеющего доступ к ключевым носителям или к ключевой информации на данных носителях, любые другие виды разглашения ключевой информации, в результате которых закрытые ключи могут стать доступными несанкционированным лицам и (или) процессам.

При компрометации ключа у Пользователя, он должен немедленно прекратить связь по сети с другими абонентами и поставить в известность Удостоверяющий Центр ООО «ИнфоЦентр» (далее – Оператор системы) о факте компрометации, с указанием особой информации (пароля), содержащейся в карточке отзыва ключа. Информация о компрометации может передаваться по телефону или непосредственно представителю Оператора в его офисе. Не позднее 1 часа после поступления сообщения о компрометации ключа, будет заблокирован ключ Пользователя в Системе. Разблокировка будет произведена только после замены скомпрометированных ключей.

Для получения новых ключей уполномоченный представитель организации-пользователя, в которой были скомпрометированы ключи, должен обратиться к Оператору системы, имея при себе документы, подтверждающие его полномочия (паспорт и две доверенности, одна из которых на получение материальных ценностей (ключевого носителя), а вторая на получение ключевых документов). За выдачу новых ключей взимается оплата в соответствии с действующими тарифами на день оплаты.