ООО «Компания «Тензор»
150001, г. Ярославль
Московский проспект, 12
(4852)262-000
www.tensor.ru

ИНН 7605016030 / КПП 760401001
р/с 40702810502910000075
в «АЛЬФА-БАНК» (ОАО) г. Ярославль
к/с 30101810200000000593
БИК 044525593

ПРАВИЛА

использования средств криптографической защиты информации и электронной подписи

1. Общие положения

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

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

2. 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 и карточки отзыва ключей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации и паролей отзыва ключей.

Пользователь несет ответственность за то, чтобы на компьютере, на котором установлены СКЗИ и средства ЭП, не были установлены и не эксплуатировались программы (в том числе, - 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 должны быть организованы мероприятия по анализу и ликвидации негативных последствий данного нарушения.

Организация - обладатель конфиденциальной информации обязана вести журнал поэкземплярногоучета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов в соответствии с п. 26 Приказа ФАПСИ от 13 июня 2001 года № 152 «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»(Приложение 2).

Не допускается:

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

б) вставлять ключевой носитель в дисковод ПЭВМ при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной подписи и т.д.), а также в дисководы других ПЭВМ;

в) записывать на ключевом носителе постороннюю информацию;

г) вносить какие-либо изменения в программное обеспечение СКЗИ и средств ЭП;

д) 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.

Пользователь самостоятельно должен определить факт компрометации закрытого ключа и оценить значение этого события для Пользователя. Мероприятия по розыску и локализации последствий компрометации конфиденциальной информации, переданной с использованием СКЗИ, организует и осуществляет сам Пользователь.

При компрометации ключа у Пользователя, он должен немедленно поставить в известность ООО «Компания «Тензор» о факте компрометации. Информация о компрометации может передаваться по телефону или непосредственно представителю Удостоверяющего центра 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, у которой были скомпрометированы ключи, должен обратиться в Удостоверяющий центр, имея при себе документы, необходимые для выпуска нового ключа ЭП. За выдачу новых ключей взимается оплата в соответствии с действующими тарифами на день оплаты.